Industrial Fast Ethernet Switch

Manual IE-SW-VL08M Series

First Edition, January 2011

1243130000/00/01.11

Weidmüller

Industrial Ethernet Switch
Manual IE-SW-VL08M Series

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Copyright © 2010 Weidmüller Interface GmbH &Co. KG.
All rights reserved.
Reproduction without permission is prohibited.

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Weidmüller.
Weidmüller provides this document “as is,” without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Weidmüller reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Weidmüller assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Contact Information

Weidmüller Interface GmbH & Co. KG
Postbox 3030
32760 Detmold
Klingenbergstraße 16
32758 Detmold
Germany

Phone: +49(0) 5231 14-0
Fax:+49(0) 5231 14-2083
E-Mail info@weidmueller.com
Internet www.weidmueller.com

Table of Contents

Chapter 1 Introduction 1-1
Overview 1-2
Package Checklist 1-2
Features 1-2

Chapter 2 Getting Started 2-1
RS-232 Console Configuration (115200, None, 8, 1, VT100) 2-2
Configuration Using a Telnet Console 2-5
Configuration Using a Web Browser 2-7
Disabling Telnet and Browser Access 2-9

Chapter 3 Featured Functions 3-1
Configuring Basic Settings 3-1
System Identification 3-1
Password 3-2
Accessible IP 3-3
Port 3-4
Network 3-5
Time 3-8
Turbo Ring DIP Switch 3-10
System File Update: By Remote TFTP 3-13
System File Update: By Local Import/Export 3-14
System File Update: By Backup Media 3-15
Restart 3-15
Factory Default 3-15
Configuring SNMP 3-16
SNMP Read/Write Settings 3-17
Trap Settings 3-19
Private MIB information 3-20
Using Communication Redundancy 3-20
The Turbo Ring Concept 3-21
Configuring “Turbo Ring” and “Turbo Ring V2” 3-25
The Turbo Chain Concept 3-31
Configuring “Turbo Chain” 3-32
The STP/RSTP Concept 3-33
Configuring STP/RSTP 3-38
Using Traffic Prioritization 3-41
The Traffic Prioritization Concept 3-41
Configuring Traffic Prioritization 3-44
Using Virtual LANs 3-46
The Virtual LAN (VLAN) Concept 3-46
Sample Applications of VLANs using the IE-SW-VL-08M 3-49
Configuring Virtual LAN 3-50
Using Multicast Filtering 3-52
The Concept of Multicast Filtering 3-52
Configuring IGMP Snooping 3-55
Static Multicast MAC 3-57
Configuring GMRP 3-58

GMRP Table 3-58
Using Rate Limiting 3-58
Configuring Rate Limiting 3-59
Using Auto Warning 3-60
Configuring Email Warning 3-60
Email Warning Events Settings 3-61
Email Settings 3-62
Configuring Relay Warning 3-63
Relay Warning Events Settings 3-64
Relay Warning List 3-65
Using Line-Swap-Fast-Recovery 3-65
Configuring Line-Swap Fast Recovery 3-66
Using Set Device IP 3-66
Configuring Set Device IP 3-67
Using Diagnosis 3-69
Mirror Port 3-69
Ping 3-70
LLDP 3-70
Using the Monitor 3-72
Monitor by Switch 3-72
Monitor by Port 3-72
Using the MAC Address Table 3-73
Using Event Log 3-74
Using Syslog 3-74

Chapter 4 Weidmüller Switch Configuration Utility A-1
Starting Ethernet Switch Configuration Utility A-2
Broadcast Search A-2
Search by IP address A-3
Upgrade Firmware A-4
Modify IP Address A-5
Export Configuration A-5
Import Configuration A-7
Unlock the Ethernet Switch A-8

Appendix A MIB Groups A-10

Appendix B Modbus/TCP Map B-1
Modbus Information B-1

1 Introduction

Welcome to the Weidmüller Industrial Ethernet Switch IE-SW-VL08M , which is designed especially for connecting Ethernet-enabled devices in industrial field applications.

The following topics are covered in this chapter:

- **Over view**
- **Package Checklist**
- **Features**

Overview

Weidmüller Industrial Ethernet Switches come with a suite of useful maintenance and monitoring functions, and is designed to provide smooth and reliable operation in harsh industrial environments. You will find that Weidmüller Industrial Ethernet Switches establish a new industrial Ethernet benchmark. The switches are excellent for keeping automation systems running continuously, are ideal for sending status reports to help prevent system damages and losses, are a great tool for mastering your industrial Ethernet networks, and are well-suited for use with industrial device control networks.

Package Checklist

The Industrial Ethernet Switch IE-SW-VL08M is shipped with the following items:

- 1 Industrial Ethernet Switch IE-SW-VL08M
- Hardware Installation Guide
- CD-ROM with Manual and Windows Utility
- RJ45 to DB9 Console port cable
- Protective caps for unused ports

NOTE: Please notify your sales representative if any of the above items are missing or damaged.

Features

- IPv6 Ready logo awarded (IPv6 Logo Committee certified).
- DHCP Option 82 for IP address assignment with different policies.
- Modbus/TCP industrial Ethernet protocol supported.
- Turbo Ring and Turbo Chain (recovery time < 20 ms at full load) and RSTP/STP (IEEE 802.1w/D).
- IGMP snooping and GMRP for filtering multicast traffic.
- Port-based VLAN, IEEE 802.1Q VLAN, and GVRP to ease network planning.
- Supports QoS → IEEE 802.1p and TOS/DiffServ to increase determinism.
- SNMPv1/v2c/v3 for different levels of network management.
- RMON for efficient network monitoring and proactive capability.
- Bandwidth management prevents unpredictable network status.
- Port mirroring for online debugging.
- Automatic warning by exception through e-mail, relay output.
- Digital inputs to integrate sensors and alarms with IP networks.

2

Getting Started

This chapter explains how to access your Industrial Ethernet Switch for the first time. There are three ways to access the switch: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect the switch to a PC's COM port, can be used if you do not know the switch's IP address. The Telnet console and web browser connection methods can be used to access Industrial Ethernet Switches over an Ethernet LAN, or over the Internet.

The following topics are covered:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration Using a Telnet Console**
- **Configuration Using a Web Browser**
- **Disabling Telnet and Browser Access**

RS-232 Console Configuration (115200, None, 8, 1, VT100)

NOTE **Connection Caution!**

1. You **cannot** connect to the IE-SW using serial console and Telnet simultaneously.
2. You **can** connect to the IE-SW using a web browser and serial console simultaneously, or using a web browser and Telnet simultaneously.
3. **Recommendation:** When you are connecting to the IE-SW using a web browser, do NOT simultaneously connect using either a serial console or by Telnet.

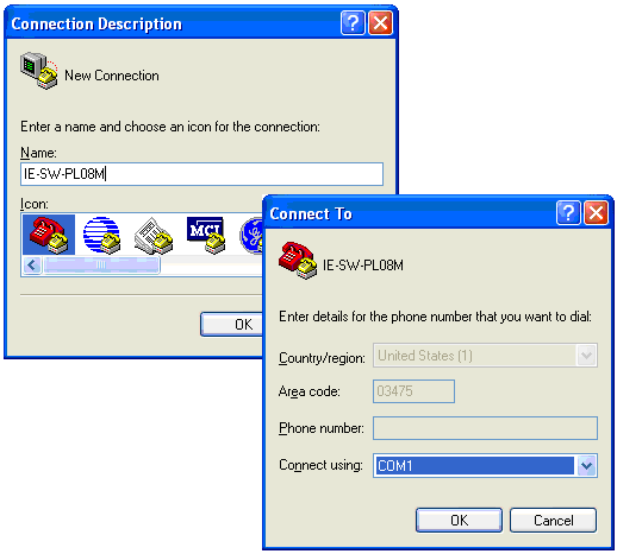
By following this advice, you can maintain better control over how your Industrial Ethernet Switch is managed.

NOTE We recommend using Hyper Terminal Tool, which is already installed under Windows XP.

Before running Hyper Terminal Tool use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the Ethernet Switch's RS-232 Console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

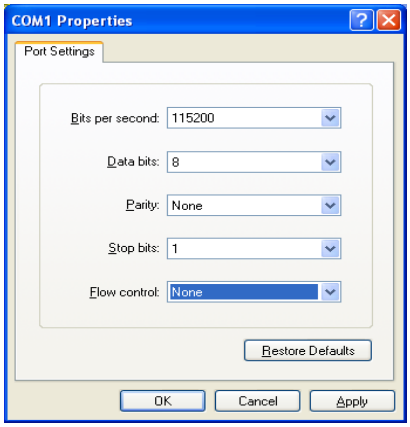
After installing Hyper Terminal Tool, do the following to access the RS-232 Console utility.

1. From the Windows desktop, click **Start → Programs → Accessories → Communications→**Hyper Terminal**.**
2. Start Hyper Terminal and enter a name of your choosing for the new connection. Select the appropriate COM port for console connection in the "New Connection" window.

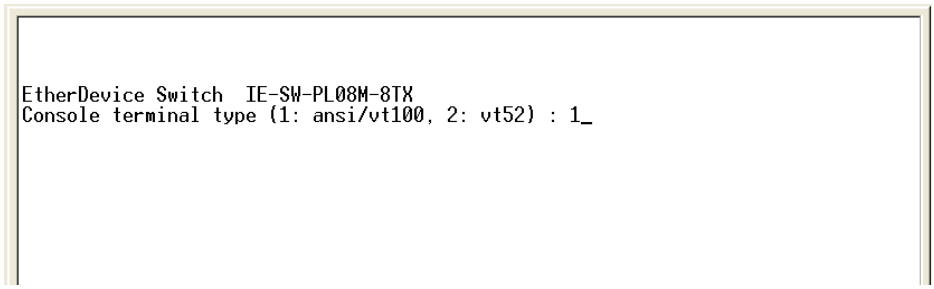


3. The Communication Parameter for console connection are:

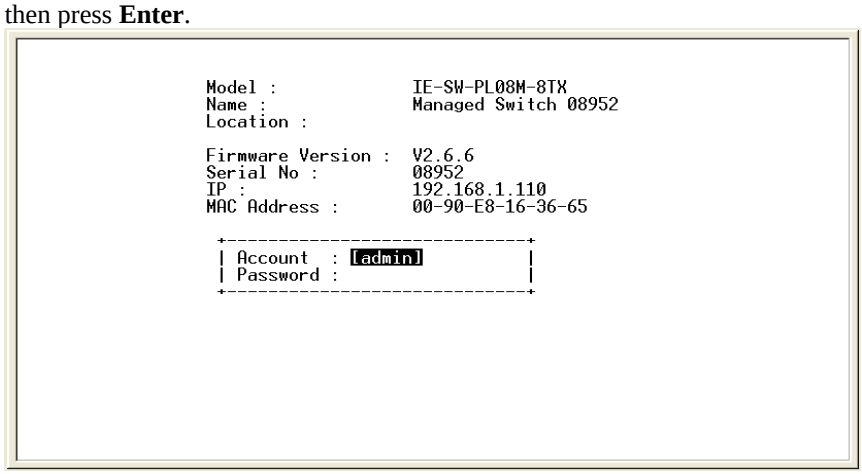
   115200 for Baud Rate, 8 for Data Bits, None for Parity, 1 for Stop bits and None for Flow Control. Click OK to continue.



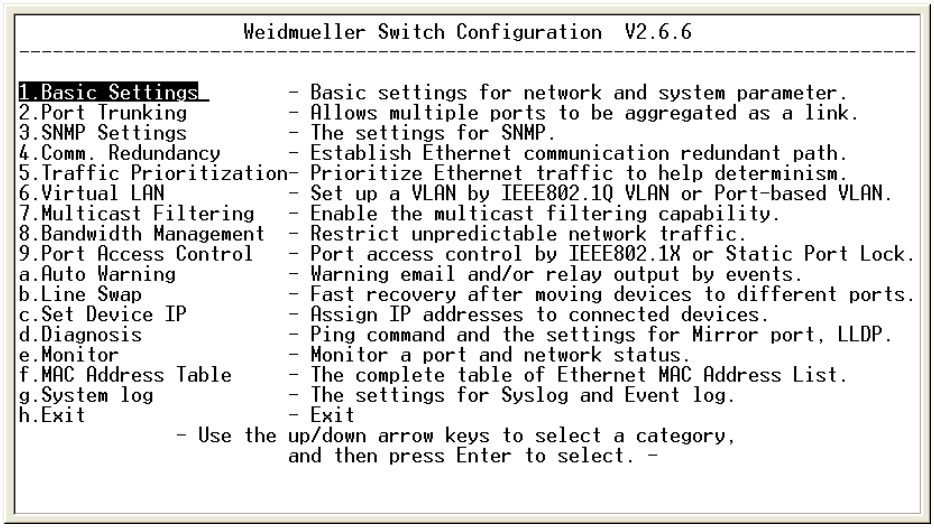
4. Type **1** to select **ansi/VT 100** terminal type, and then press **Enter**.



5. The Console login screen will appear. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor to the Password field, enter the default **Console Password "Detmold"** (this is the same as the Web Browser password; leave the **Password** field blank if a console password has not been set), and then press **Enter**.

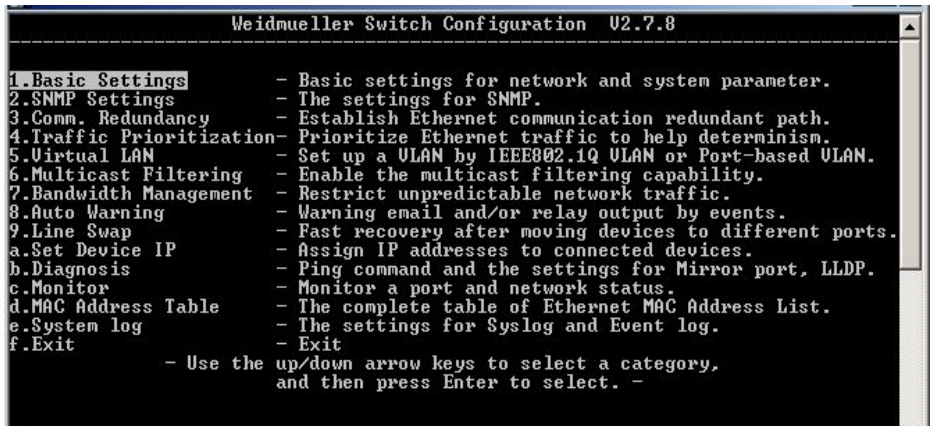


6. The IE-SW-VL08M's Main Menu will be displayed


Weidmueller Switch Configuration V2.6.6
1.Basic Settings - Basic settings for network and system parameter.
2.Port Trunking - Allows multiple ports to be aggregated as a link.
3.SNMP Settings - The settings for SNMP.
4.Comm. Redundancy - Establish Ethernet communication redundant path.
5.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
6.Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
7.Multicast Filtering - Enable the multicast filtering capability.
8.Bandwidth Management - Restrict unpredictable network traffic.
9.Port Access Control - Port access control by IEEE802.1X or Static Port Lock.
a.Auto Warning - Warning email and/or relay output by events.
b.Line Swap - Fast recovery after moving devices to different ports.
c.Set Device IP - Assign IP addresses to connected devices.
d.Diagnosis - Ping command and the settings for Mirror port, LLDP.
e.Monitor - Monitor a port and network status.
f.MAC Address Table - The complete table of Ethernet MAC Address List.
g.System log - The settings for Syslog and Event log.
h.Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -

7. The Console login screen will be displayed. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor to the Password field, enter the **Console Password** (this is the same as the Web Browser password; leave the **Password** field blank if a console password has not been set), and then press **Enter**.

8. The IE-SW-VL08M's **Main Menu** will be displayed.


Weidmueller Switch Configuration V2.7.8
1.Basic Settings - Basic settings for network and system parameter.
2.SNMP Settings - The settings for SNMP.
3.Comm. Redundancy - Establish Ethernet communication redundant path.
4.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
5.Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
6.Multicast Filtering - Enable the multicast filtering capability.
7.Bandwidth Management - Restrict unpredictable network traffic.
8.Auto Warning - Warning email and/or relay output by events.
9.Line Swap - Fast recovery after moving devices to different ports.
a.Set Device IP - Assign IP addresses to connected devices.
b.Diagnosis - Ping command and the settings for Mirror port, LLDP.
c.Monitor - Monitor a port and network status.
d.MAC Address Table - The complete table of Ethernet MAC Address List.
e.System log - The settings for Syslog and Event log.
f.Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -

NOTE Before accessing the console utility via Telnet, first connect one of the IE-SW-VL08M's RJ45 Ethernet ports to your Ethernet LAN, or connect directly to your PC's Ethernet NIC. You can establish a connection with either a straight-through or cross-over Ethernet cable. If you have difficulty connecting, refer to the Auto MDI/MDI-X Connection section from the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

9. After entering the Main Menu, use the following keys to move the cursor, and to select options.

Key	Function
Up/Down/Left/Right arrows, or Tab	Move the onscreen cursor
Enter	Display & select options
Space	Toggle options
Esc	Previous Menu

Configuration Using a Telnet Console

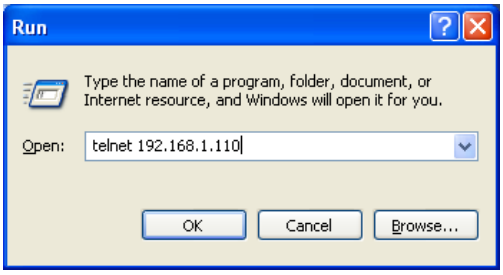
You may use Telnet to access the IE-SW-VL08M's console utility over a network. To be able to access the IE-SW-VL08M-'s functions over the network (using Telnet or a Web Browser) from a PC host that is connected to the same LAN as the IE-SW-VL08M, you need to make sure that the PC host and the IE-SW-VL08M are on the same logical sub network. To do this, check your PC host's IP address and netmask. By default, the IE-SW-VL08M's IP address is 192.168.1.110 and the netmask is 255.255.255.0 (for a Class C network). If you do not change these values, and your PC host's netmask is 255.255.255.0, then its IP address must have the form 192.168.1.xxx. On the other hand, if your PC host's netmask is 255.255.255.0, then its IP address must have the form 192.168.1.xxx.

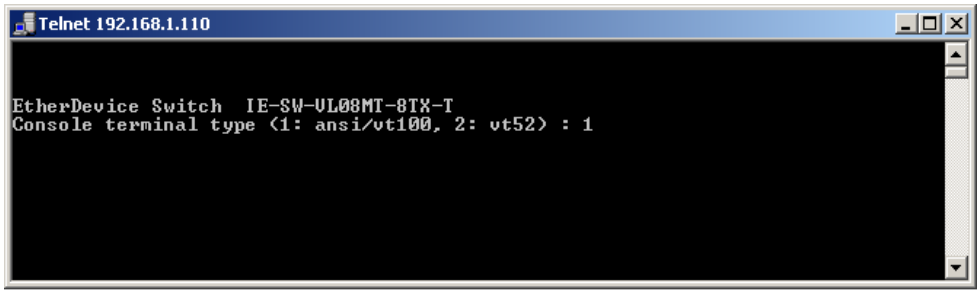
NOTE To use the IE-SW-VL08M's management and monitoring functions from a PC host connected to the same LAN as the IE-SW-VL08M', you must make sure that the PC host and the IE-SW-VL08M's are on the same logical sub network.

The IE-SW-VL08M's default IP address is 192.168.1.110.

Perform the following steps to access the console utility via Telnet.

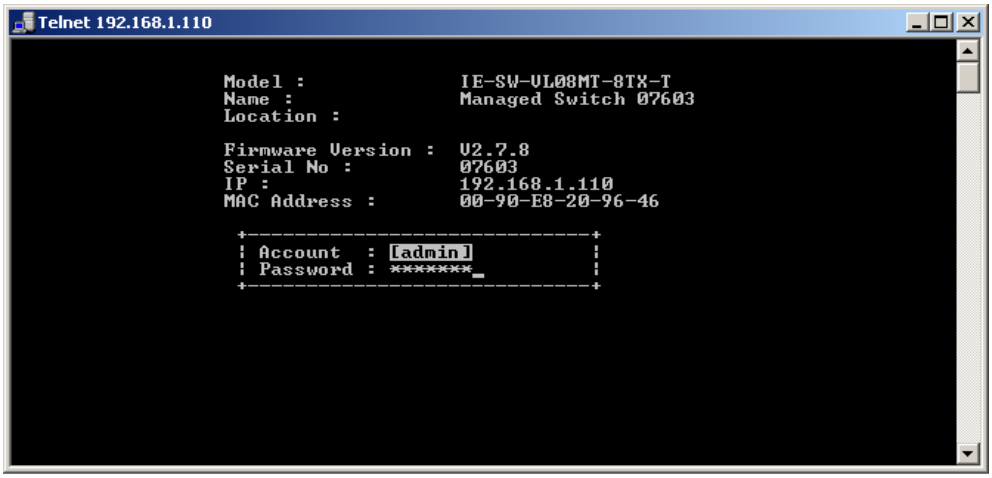
1. Telnet to the IE-SW-VL08M's IP address from the Windows **Run** window (or from the command prompt).



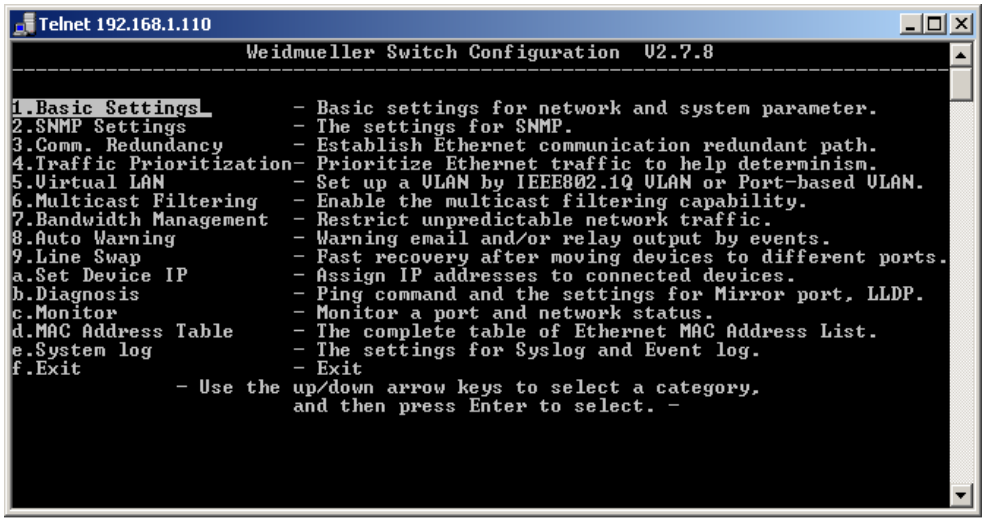


2. Type **1** to choose **ansi/vt100**, and then press **Enter**.

3. The Console login screen will be displayed. Press **Enter** to open the Account pop-up selector and then select either **admin** or **user**. Use the keyboard's down arrow to move the cursor to the Password field, enter the **Console Password** (this is the same as the Web Browser password; leave the **Password** field blank if a console password has not been set), and then press **Enter**.



4. The IE-SW-VL08M's **Main Menu** will be displayed. (**NOTE:** To modify the appearance of the PComm Terminal Emulator window, select **Font…** under the **Edit** menu, and then choose the desired formatting options.)


Telnet 192.168.1.110
Weidmueller Switch Configuration V2.7.8
1.Basic Settings - Basic settings for network and system parameter.
2.SNMP Settings - The settings for SNMP.
3.Comm. Redundancy - Establish Ethernet communication redundant path.
4.Traffic Prioritization- Prioritize Ethernet traffic to help determinism.
5.Virtual LAN - Set up a VLAN by IEEE802.1Q VLAN or Port-based VLAN.
6.Multicast Filtering - Enable the multicast filtering capability.
7.Bandwidth Management - Restrict unpredictable network traffic.
8.Auto Warning - Warning email and/or relay output by events.
9.Line Swap - Fast recovery after moving devices to different ports.
a.Set Device IP - Assign IP addresses to connected devices.
b.Diagnosis - Ping command and the settings for Mirror port, LLDP.
c.Monitor - Monitor a port and network status.
d.MAC Address Table - The complete table of Ethernet MAC Address List.
e.System log - The settings for Syslog and Event log.
f.Exit - Exit
- Use the up/down arrow keys to select a category,
and then press Enter to select. -

NOTE	The Telnet Console looks and operates in precisely the same manner as the RS-232 Console.

Configuration Using a Web Browser

The IE-SW-VL08M's web browser interface provides a convenient way to modify the switch's configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft Internet Explorer 5.5 or 6.0 with JVM (Java Virtual Machine) installed.

NOTE	To use the Ethernet Switch's management and monitoring functions from a PC host connected to the same LAN as the IE-SW-VL08M', you must make sure that the PC host and the Ethernet switch are on the same logical sub network.

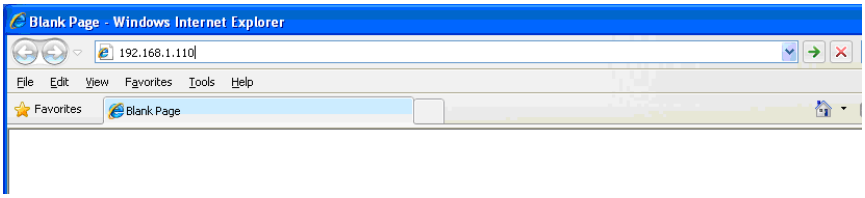
NOTE	If the Ethernet Switch is configured for other VLAN settings, you must make sure your PC host is on the Management VLAN.

NOTE	Before accessing the IE-SW-VL08M's web browser interface, first connect one of the device's RJ45 Ethernet ports to your Ethernet LAN, or directly to your PC's Ethernet NIC. You can establish a connection with either a straight-through or cross-over Ethernet cable. If you have difficulty connecting, refer to the Auto MDI/MDI-X Connection section from the Hardware installation Guide for more information about the different types of Ethernet cables and ports.

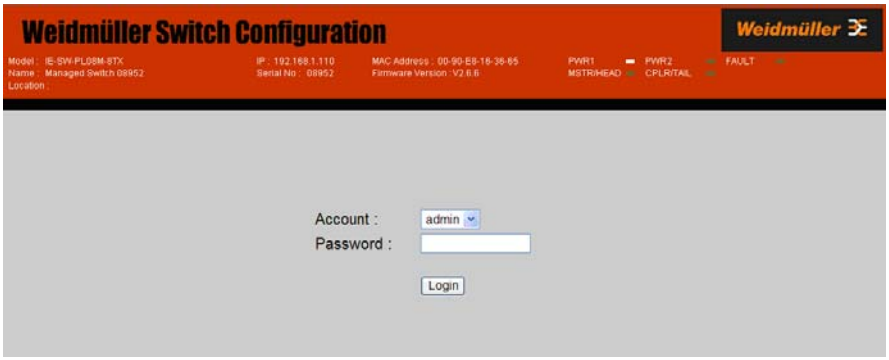
NOTE	**The IE-SW-VL08M's default IP is 192.168.1.110.**

Perform the following steps to access the web browser interface.

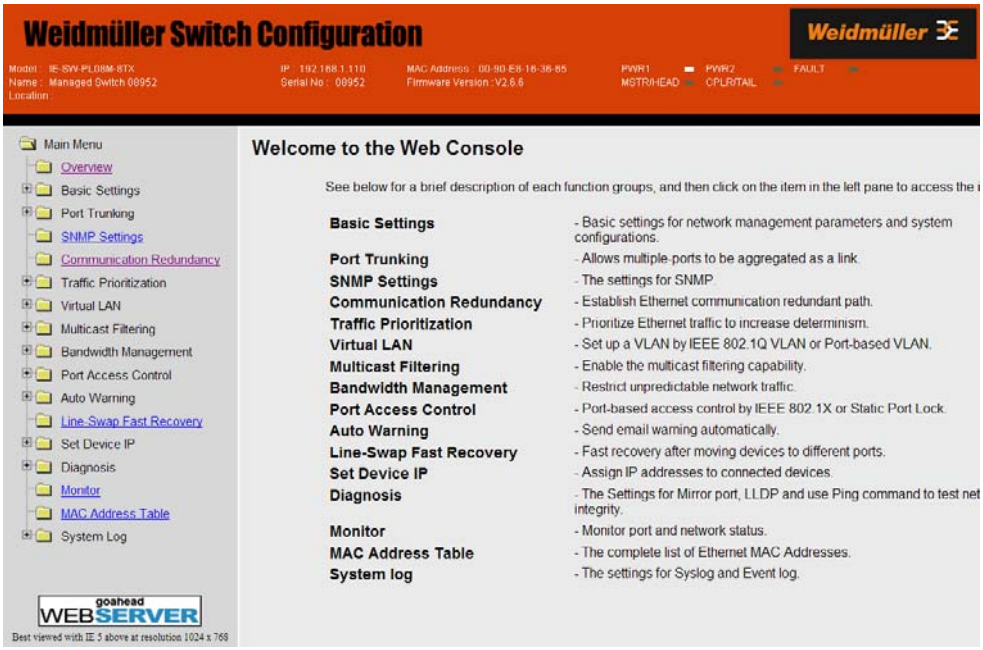
1. Open Internet Explorer and type the IE-SW-VL08M's IP address in the **Address** field. Press **Enter** to establish the connection.



2. The web login page will be displayed. Select the login account (Admin or User) and enter the **Password** (this is the same as the Console password), and then click **Login** to continue. Leave the **Password** field blank if a password has not been set.

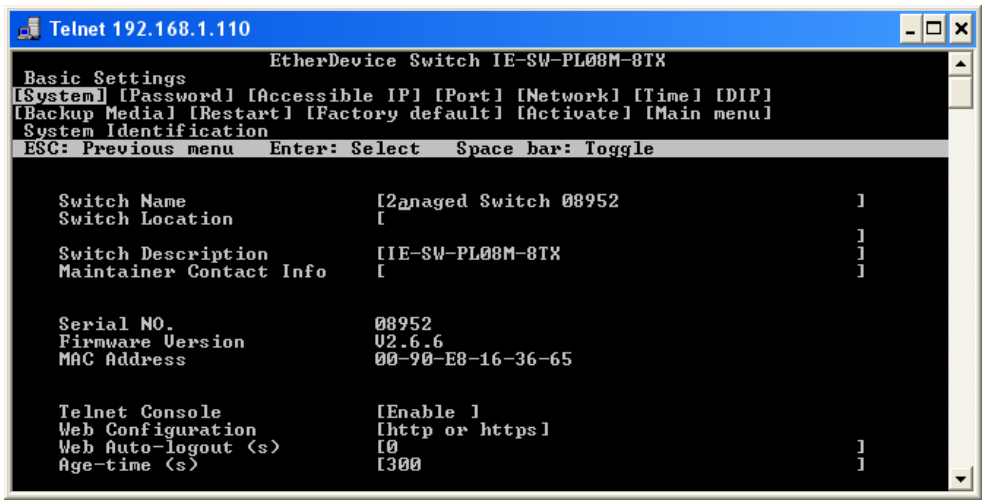


You may need to wait a few moments for the web page to be downloaded to your computer. Use the menu tree on the left side of the window to open the function pages to access each of the Ethernet switch functions.


Weidmüller Switch Configuration
Weidmüller
Main Menu
Overview
Basic Settings
Port Trunking
SNMP Settings
Communication Redundancy
Traffic Prioritization
Virtual LAN
Multicast Filtering
Bandwidth Management
Port Access Control
Auto Warning
Line-Swap Fast Recovery
Set Device IP
Diagnosis
Monitor
MAC Address Table
System Log
goahead WEBSERVER
Welcome to the Web Console
See below for a brief description of each function groups, and then click on the item in the left pane to access the
Basic Settings - Basic settings for network management parameters and system configurations.
Port Trunking - Allows multiple ports to be aggregated as a link.
SNMP Settings - The settings for SNMP.
Communication Redundancy - Establish Ethernet communication redundant path.
Traffic Prioritization - Prioritize Ethernet traffic to increase determinism.
Virtual LAN - Set up a VLAN by IEEE 802.1Q VLAN or Port-based VLAN.
Multicast Filtering - Enable the multicast filtering capability.
Bandwidth Management - Restrict unpredictable network traffic.
Port Access Control - Port-based access control by IEEE 802.1X or Static Port Lock.
Auto Warning - Send email warning automatically.
Line-Swap Fast Recovery - Fast recovery after moving devices to different ports.
Set Device IP - Assign IP addresses to connected devices.
Diagnosis - The Settings for Mirror port, LLDP and use Ping command to test net integrity.
Monitor - Monitor port and network status.
MAC Address Table - The complete list of Ethernet MAC Addresses.
System log - The settings for Syslog and Event log.

Disabling Telnet and Browser Access

If you are connecting the IE-SW-VL08M to a public network, but do not intend to use its management functions over the network, then we suggest disabling both **Telnet Console** and **Web Configuration** from the RS-232 Console's **Basic Settings → System Identification** page, as shown in the following figure.


Telnet 192.168.1.110
EtherDevice Switch IE-SW-PL08M-8TX
Basic Settings
[System] [Password] [Accessible IP] [Port] [Network] [Time] [DIP]
[Backup Media] [Restart] [Factory default] [Activate] [Main menu]
System Identification
ESC: Previous menu Enter: Select Space bar: Toggle
Switch Name [2naged Switch 08952]
Switch Location [ ]
Switch Description [IE-SW-PL08M-8TX]
Maintainer Contact Info [ ]
Serial NO. 08952
Firmware Version V2.6.6
MAC Address 00-90-E8-16-36-65
Telnet Console [Enable]
Web Configuration [http or https]
Web Auto-logout (s) [0]
Age-time (s) [300]

NOTE If you are connecting the IE-SW-VL08M to a public network, but do not intend to use its management functions over the network, then we suggest disabling both **Telnet Console** and **Web Configuration**.

3

Featured Functions

This chapter explains how to access a Weidmueller Ethernet switch's various configuration, monitoring, and administration functions. There are three ways to access these functions: serial console, Telnet console, and web browser. The serial console connection method, which requires using a short serial cable to connect the switch to a PC's COM port, can be used if you do not know the IE-SW's IP address. The Telnet console and web browser connection methods can be used to access the IE-SW over an Ethernet LAN, or over the Internet.

The Web Console is the most user-friendly way to configure your Ethernet Switch. In this chapter, we use the Web Console interface to introduce the device functions. There are only a few differences between the Web Console, Serial Console, and Telnet Console access methods.

The following topics are covered in this chapter:

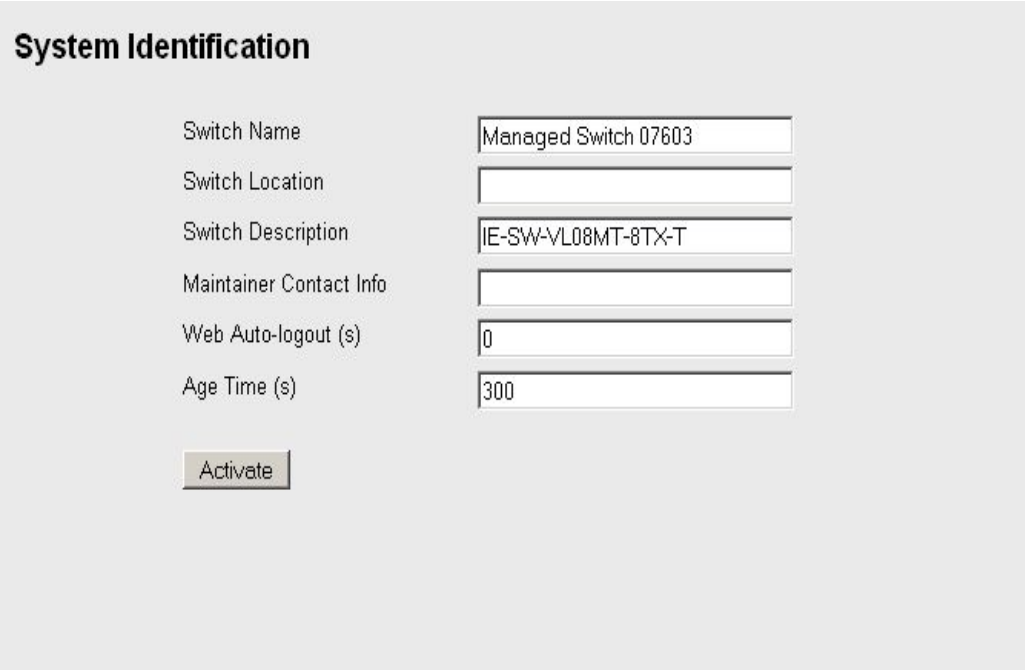
- ☐ **Configuring Basic Settings**
- ☐ **Configuring Basic Settings**
- ☐ **Network**
- ☐ **Configuring SNMP**
- ☐ **Using Communication Redundancy**
- ☐ **Using Traffic Prioritization**
- ☐ **Using Virtual LANs**
- ☐ **Using Multicast Filtering**
- ☐ **Using Rate Limiting**
- ☐ **Using Auto Warning**
- ☐ **Using Line-Swap-Fast-Recovery**
- ☐ **Using Set Device IP**
- ☐ **Using Diagnosis**
- ☐ **Using the Monitor**
- ☐ **Using the MAC Address Table**
- ☐ **Using Event Log**
- ☐ **Using Syslog**

Configuring Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the Ethernet Switch.

System Identification

The system identification items are displayed at the top of the web page, and will be included in alarm emails. Setting system identification items makes it easier to identify the different switches connected to your network.



Switch Name

Setting	Description	Factory Default
Max. 30 Characters	This option is useful for specifying the role or application of different IE-Switch units. E.g., Factory Switch 1.	Industrial Ethernet Switch [*Serial No. of this switch*]

Switch Location

Setting	Description	Factory Default
Max. 80 Characters	To specify the location of different IE-Switch units. E.g., production line 1.	Switch Location

Switch Description

Setting	Description	Factory Default
Max. 30 Characters	Use this to record a more detailed description of the Ethernet switch.	*None*

Maintainer Contact Info

Setting	Description	Factory Default

Max.30 Characters	Use this to record contact information of the person responsible for maintaining this IE-SW-VL08M switch.	*None*

Web Configuration

Setting	Description	Factory Default
Disable / http or https / https only	You can select disable, or accept both http and https, or https only, from the web console	*http or https*

Web Auto-logout (s)

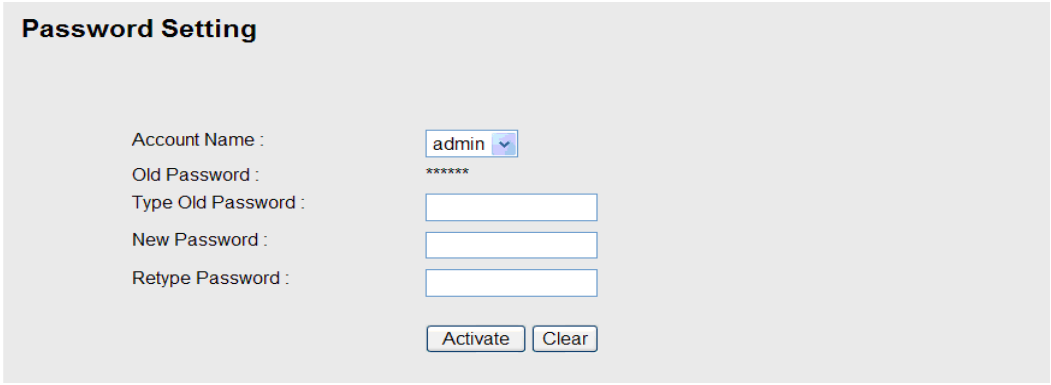
Setting	Description	Factory Default
60 to 86400 (seconds)	Disable or extend the auto-logout time for the web management console.	*0 (disable)*

Age time (s)

Setting	Description	Factory Default
15 to 3825 (seconds)	The length of time that a MAC address entry can remain in the Weidmueller switch. When an entry reaches its aging time, it "ages out" and is purged from the switch, effectively cancelling frame forwarding to that specific port.	*300*

Password

The Weidmueller switch provides two levels of access privileges: **admin** privilege gives read/write access to all switch configuration parameters; **user** privilege provides read access only—you will be able to view the configuration, but will not be able to make modifications.



ATTENTION

The IE-SW-VL08M's default Password is set to "Detmold".
If a Password is set, then you will be required to type the Password when logging into the RS-232 Console, Telnet Console, or Web Browser interface.

Account

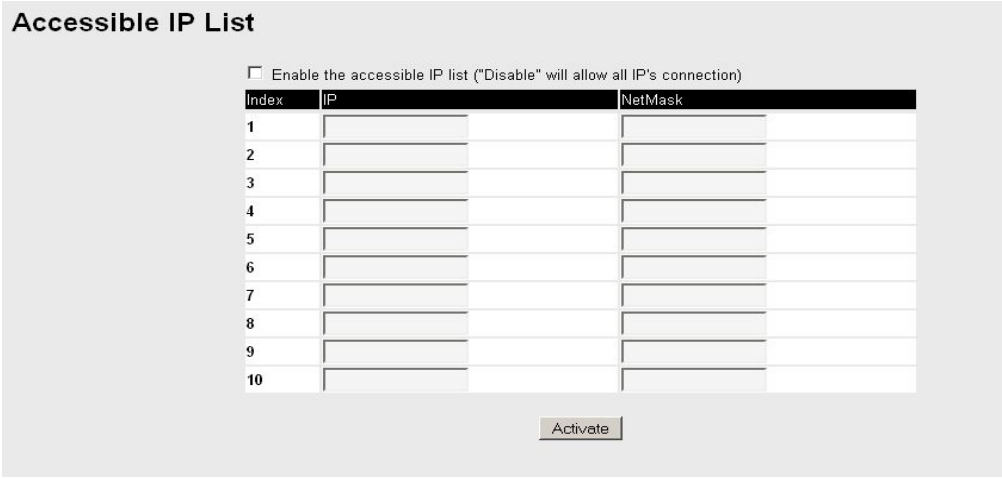
Setting	Description	Factory Default
admin	***admin*** privilege allows the user to modify all device configurations.	admin
user	***user*** privilege only allows viewing device configurations.	

Password

Setting	Description	Factory Default
Old Password (Max. 16 Characters)	Type current password when changing the password	*None*
New Password **(**Max. 16 Characters)	Type new password when changing the password	*None*
Retype Password (Max. 16 Characters)	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	*None*

Accessible IP

An IP address-based filtering method to control access to Weidmueller switches.



Accessible IP Settings allows you to add or remove ***Legal*** remote host IP addresses to prevent unauthorized access. Access to the Weidmueller switch is controlled by IP addresses. That is, if a host's IP address is in the accessible IP table, then the host will be allowed access to the device. You can allow one of the following cases by setting this parameter

- **Only one host with the specified IP address can access the IE-SW-VL08M**
  E.g., enter "192.168.1.1/255.255.255.255" to allow access to *just* the IP address 192.168.1.1.
- **Any host on a specific sub network can access the IE-SW-VL08M**
  E.g., enter "192.168.1.0/255.255.255.0" to allow access to all IPs on the sub network defined by this IP address/netmask combination.

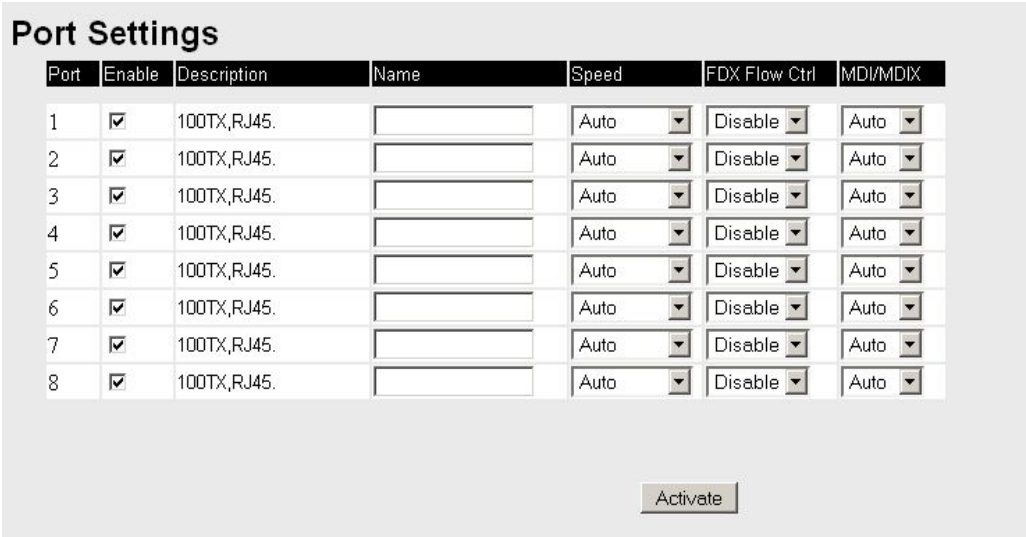
- **Any host can access the IE-SW-VL08M**
  Disable this function by not selecting the ***Enable the accessible IP list*** checkbox.

  The following table shows additional configuration examples:

Allowable Hosts	Input format
Any host	Disable
192.168.1.120	192.168.1.120 / 255.255.255.255
192.168.1.1 to 192.168.1.254	192.168.1.0 / 255.255.255.0
192.168.0.1 to 192.168.255.254	192.168.0.0 / 255.255.0.0
192.168.1.1 to 192.168.1.126	192.168.1.0 / 255.255.255.128
192.168.1.129 to 192.168.1.254	192.168.1.128 / 255.255.255.128

Port

Port settings are included to give the user control over Port Access, Port Transmission Speed, Flow Control, and Port Type (MDI or MDIX). An explanation of each configuration item is given below. (NOTE: The user interface for the **IE-SW-VL08M** will show 8 ports.)



Enable

Setting	Description	Factory Default
checked	Allows data transmission through the port.	disabled
unchecked	Immediately shuts off port access.	

ATTENTION

If a connected device or sub-network is wreaking havoc on the rest of the network, the **Disable** option under **Advanced Settings/Port** gives the administrator a quick way to immediately shut off access through this port.

Name

Setting	Description	Factory Default
Max. 63 Characters	Specify an alias for each port, and assist the administrator in remembering important information about the port. E.g., PLC 1	*None*

Port Transmission Speed

Setting	Description	Factory Default
Auto	Allows the port to use the IEEE 802.3u protocol to negotiate with connected devices. The port and connected devices will determine the best speed for that connection.	Auto
100M-Full	Choose one of these fixed speed options if the Ethernet device at the other end has trouble auto-negotiating for line speed.	
100M-Half		
10M-Full		
10M-Half		

FDX Flow Control

This setting enables or disables the flow control capability of this port when the ***port transmission speed*** setting is on ***auto*** mode. The final result will be determined by the ***auto*** process between the IE-SW-VL08M and the connected device.

Setting	Description	Factory Default
Enable	Enables the flow control capability of this port when in auto-nego mode.	Disable
Disable	Disables the flow control capability of this port when in auto-nego mode.	

Port Type

Setting	Description	Factory Default
Auto	Allows the port to auto detect the port type of the Ethernet device at the other end and change the port type accordingly.	Auto
MDI	Choose the MDI or MDIX option if the Ethernet device at the other end has trouble auto-negotiating for port type.	
MDIX		

Network

The **Network** configuration allows users to configure both IPv4 and IPv6 parameters for management access over the network. The IE-SW-VLxxM series supports both IPv4 and IPv6, and can be managed through either of these address types.

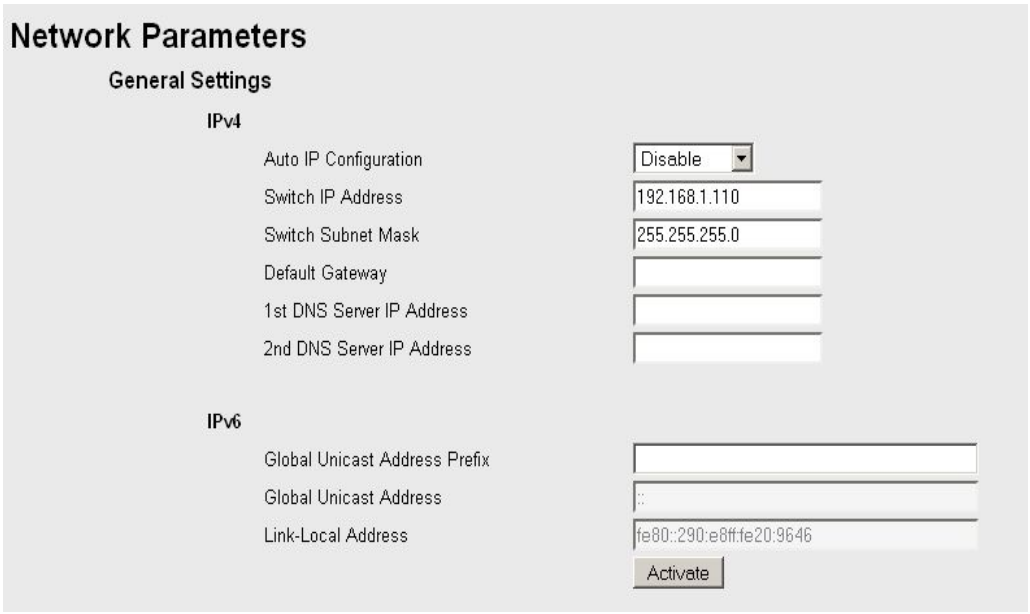
IPv4

The IPv4 settings include the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server.

IPv6

IPv6 setting includes two distinct address types—Link-Local Unicast address and Global Unicast address. A Link-Local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. To connect to a larger network with multiple segments, the switch must be configured with a Global Unicast address.

See a brief explanation of each configuration item below.



Auto IP Configuration

Setting	Description	Factory Default
Disable	Set up the IE-SW-VL08M's IP address manually.	Disable
By DHCP	The IP address will be assigned automatically by the network's DHCP server.	
By BOOTP	The IP address will be assigned automatically by the network's BOOTP server.	

Switch IP Address

Setting	Description	Factory Default
IP Address of the IE-SW-VL08M	Identifies the IE-SW-VL08M on a TCP/IP network.	192.168.127.253

Switch Subnet Mask

Setting	Description	Factory Default
Subnet mask of the IE-SW-VL08M	Identifies the type of network to which the IE-SW-VL08M is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

Default Gateway

Setting	Description	Factory Default
Default Gateway of the IE-SW-VL08M	The IP address of the router that connects the LAN to an outside network.	*None*

DNS IP Address

Setting	Description	Factory Default
1st DNS Server's IP Address	The IP address of the DNS Server used by your network.	*None*
2nd DNS Server's IP Address	The IP address of the DNS Server used by your network. The IE-SW-VL08M will try to locate the 2nd DNS Server if the 1st DNS Server fails to connect.	*None*

Global Unicast Address Prefix (Prefix Length: 64 bits)

Setting	Description	Factory Default
Global Unicast Address Prefix	The prefix value must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.	*None*

Global Unicast Address

Setting	Description	Factory Default
None	Displays the IPv6 Global Unicast address. The network portion of the Global Unicast address can be configured by specifying the Global Unicast Prefix and using a EUI-64 interface ID in the low order 64 bits. The host portion of the Global Unicast address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address)	None

Link-Local Address

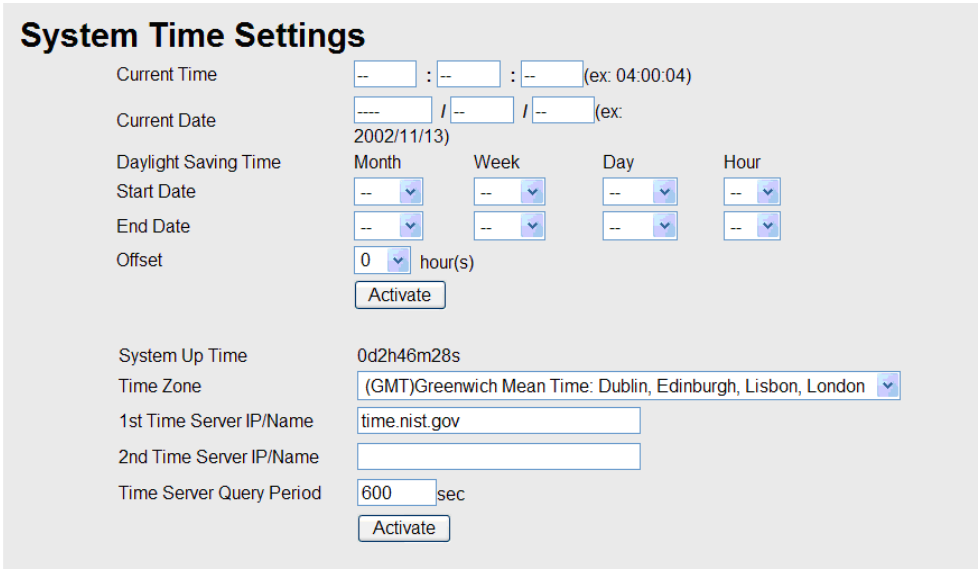
Setting	Description	Factory Default
None	The network portion of the Link-Local address is FE80 and the host portion of Link-Local address is automatically generated using the modified EUI-64 from of the interface identifier (Switch's MAC address)	FE80: (EUI-64 form of the MAC address)

Neighbor Cache

Setting	Description	Factory Default
None	The information in the neighbor cache that includes the neighboring node's IPv6 address, the corresponding Link-Layer address, and the current state of the entry.	*None*

Time

The **Time** configuration page lets users set the time, date, and other settings. An explanation of each setting is given below the figure.



The switch has a time calibration function based on information from an NTP server or user specified Time and Date information. Functions such as Auto warning ***Email*** can add real-time information to the message.

NOTE The IE-SW-VL08M does not have a real time clock. The user must update the **Current Time** and **Current Date** to set the initial time for the device after each reboot, especially when the network does not have an Internet connection for NTP server or there is no NTP server on the LAN.

Current Time

Setting	Description	Factory Default

User adjustable time.	The time parameter allows configuration of the local time in local 24-hour format.	*None* (hh:mm:ss)

Current Date

Setting	Description	Factory Default
User adjustable date.	The date parameter allows configuration of the local date in yyyy/mm/dd format.	*None* (yyyy/mm/dd)

Daylight Saving Time

Daylight saving time (also know as **DST** or **summer time**) involves advancing clocks (usually 1 hour) during the summer time to provide an extra hour of daylight in the afternoon.

Start Date

Setting	Description	Factory Default
User adjustable date.	The Start Date parameter allows users to enter the date that daylight saving time begins.	None

End Date

Setting	Description	Factory Default
User adjustable date.	The End Date parameter allows users to enter the date that daylight saving time ends.	None

Offset

Setting	Description	Factory Default
User adjustable hour.	The offset parameter indicates how many hours forward the clock should be advanced.	None

System Up Time

Indicates the switch's up time from the last cold start. The unit is seconds.

Time Zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

NOTE Changing the time zone will automatically correct the current time. You should **configure the time zone before setting the time**.

Time Server IP/Name

Setting	Description	Factory Default
1st Time Server IP/Name	IP or Domain address (e.g., 192.168.1.1 or time.nist.gov)	None
2nd Time Server IP/Name	The device will try to locate the 2nd NTP Server if the connection to the 1st NTP server failed.	

Time Server Query Period

Setting	Description	Factory Default
Query Period	This parameter determines how frequently the time is updated from the NTP server.	600 seconds

Turbo Ring DIP Switch

The **Turbo Ring DIP Switch** page allows users to disable the four DIP switches located on the switch's outer casing. When enabled, the DIP switches can be used to configure basic settings for either the "Turbo Ring" protocol or "Turbo Ring V2" protocol. A complete description of the settings is given below.

NOTE The "Turbo Ring" protocol (recovery time < 300 ms) provides better network reliability and faster recovery time for redundant ring topologies. The "Turbo Ring V2" protocol (recovery time < 20 ms), supports additional redundant ring architectures.

In this manual, we use the terminology ***"Turbo Ring" ring*** and ***"Turbo Ring V2" ring*** to differentiate between rings configured for one or the other of these protocols.

For a detailed description of "Turbo Ring" and "Turbo Ring V2," please refer to the **Using Communication Redundancy** section later in this chapter.

How to Enable or Disable the Turbo Ring DIP Switches

Turbo Ring DIP Switch
Disable the Turbo Ring DIP Switch
1. To enable the entire set of Hardware DIP switches, uncheck the "Disable the Turbo Ring DIP Switch" option.
2. To disable the entire set of Hardware DIP switches, check the "Disable the Turbo Ring DIP Switch" option.
Set DIP switch as Turbo Ring
Set DIP switch as Turbo Ring V2
Activate

Enable / Disable the Turbo Ring DIP Switch

Setting	Description	Factory Default
Enable the Turbo Ring DIP Switches	The four DIP switches are *enabled* when the "Disable the Turbo Ring DIP Switch" box is not checked.	Not checked (i.e., the Turbo Ring DIP Switches are enabled by default)
Disable the Turbo Ring DIP Switches	The four DIP switches are *disabled* when the "Disable the Turbo Ring DIP Switch" box is checked.	

Set DIP switch as Turbo Ring / Set DIP switch as Turbo Ring V2

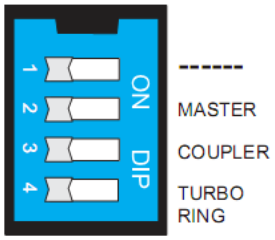
Setting	Description	Factory Default
Set DIP switch as Turbo Ring	Select this option to enable the Turbo Ring DIP switches to configure the device for a "Turbo Ring" ring.	This is the default if you do NOT reset the switch to factory default settings (provided you upgraded the firmware for Turbo Ring V2).
Set DIP switch as Turbo Ring V2	Select this option to enable the Turbo Ring DIP switches to configure the device for a "Turbo Ring V2" ring.	This is the default if you DO reset the switch to factory default settings (provided you upgraded the firmware for Turbo Ring V2).

NOTE If you upgrade the firmware of your IE-SW-VL08M from Turbo Ring to Turbo Ring V2, but do not reset the switch to factory defaults, the DIP switches will be set to configure the device for a "Turbo Ring" ring. If you reset the switch to factory defaults, the DIP switches will be set to configure the device for a "Turbo Ring V2" ring.

How to Configure the Turbo Ring DIP Switches

The Turbo Ring DIP Switches are set to the OFF position at the factory.

NOTE The four DIP Switches are used to configure both the "Turbo Ring" and "Turbo Ring V2" protocols, depending on which protocol is active. To select which protocol the switch will use, start the user interface software, and then use the left menu to navigate to the **Communication Redundancy** page. To use one of the Turbo Ring protocols for the switch, select either "Turbo Ring" or "Turbo Ring V2" in the **Redundancy Protocol** drop-down box. See the **Configuring "Turbo Ring" and "Turbo Ring V2"** section in this chapter for details.



The following tables show how to use the DIP switches to configure the switch for "Turbo Ring" or "Turbo Ring V2."

NOTE DIP switch 4 must be set to the ON position to enable DIP switches 1, 2, and 3. If DIP switch 4 is set to the "OFF" position, then DIP switches 1, 2, and 3 will all be disabled.

"Turbo Ring" DIP Switch Settings

DIP 1	DIP 2	DIP 3	DIP 4
Reserved for future use.	ON: Enables this switch as the Ring Master.	ON: Enables the default "Ring Coupling" ports.	ON: Activates DIP switches 1, 2, 3 to configure "Turbo Ring" settings.
	OFF: This switch will not be the Ring Master.	OFF: Do not use this switch as the ring coupler.	OFF: DIP switches 1, 2, 3 will be disabled.

"Turbo Ring V2" DIP Switch Settings

DIP 1	DIP 2	DIP 3	DIP 4
ON: Enables the default "Ring Coupling (backup)" port.	ON: Enables this switch as the Ring Master.	ON: Enables the default "Ring Coupling" port.	ON: Activates DIP switches 1, 2, 3 to configure "Turbo Ring V2" settings.
OFF: Enables the default "Ring Coupling (primary)" port.	OFF: This switch will not be the Ring Master.	OFF: Do not use this switch as a ring coupler.	OFF: DIP switches 1, 2, 3 will be disabled.

NOTE The DIP 1 setting will only be active if DIP 3 is in the ON position. If you set DIP 3 to OFF, then the default Ring Coupling port will NOT be enabled, even if DIP 1 is ON.

Protocol	Default Turbo Ring Ports	Default Ring Coupling Port(s)
Turbo Ring	Ports 4 and 5 Ports 7 and 8	Ports 2 and 3 Ports 5 and 6
Turbo Ring V2	Ports 4 and 5 Ports 7 and 8	Port 2 Port 5

NOTE The Turbo Ring Ports and Coupling Ports will be added automatically to all VLANs if you set DIP Switch 4 to the "ON" position.

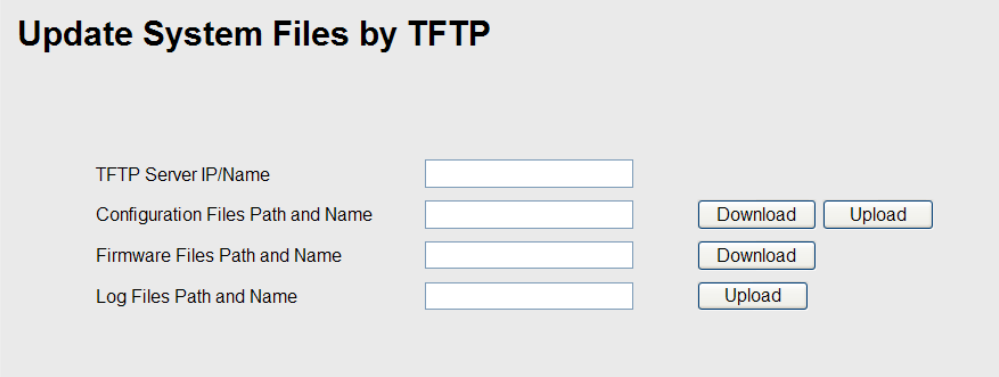
NOTE If you do not enable any of the IE-SW-VL08M switches to be the Ring Master, the Turbo Ring protocol will automatically choose the IE-SW-VL08M with the smallest MAC address range to be

the Ring Master. If you accidentally enable more than one IE-SW-VL08M to be the Ring Master, these IE-SW-VL08M switches will auto-negotiate to determine which one will be the Ring Master.

NOTE If you use the browser interface to enable the DIP switches (by un-checking the "Disable the Turbo Ring DIP switch" checkbox), and then flip DIP switch 4 from **ON** to **OFF**, the Ring Ports and Coupling Ports that were added to all VLANs will be restored to their previous software settings. (For details, please refer to the "Using Virtual LANs" section of this manual).

System File Update: By Remote TFTP

The IE-SW-VL08M supports saving your configuration file to a remote TFTP server or local host to allow other IE-SW-VL08M switches to use the same configuration at a later time, or saving the Log file for future reference. Loading pre-saved firmware or a configuration file from the TFTP server or local host is also supported for easy upgrading or configuration of the device.



TFTP Server IP/Name

Setting	Description	Factory Default
IP Address of the TFTP Server	The IP or name of the remote TFTP server. Must be set up before downloading or uploading files.	None

Configuration Files Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the device's configuration file on the TFTP server.	None

Firmware Files Path and Name

Setting	Description	Factory Default
Max. 40 Characters	The path and file name of the devices's firmware file.	None

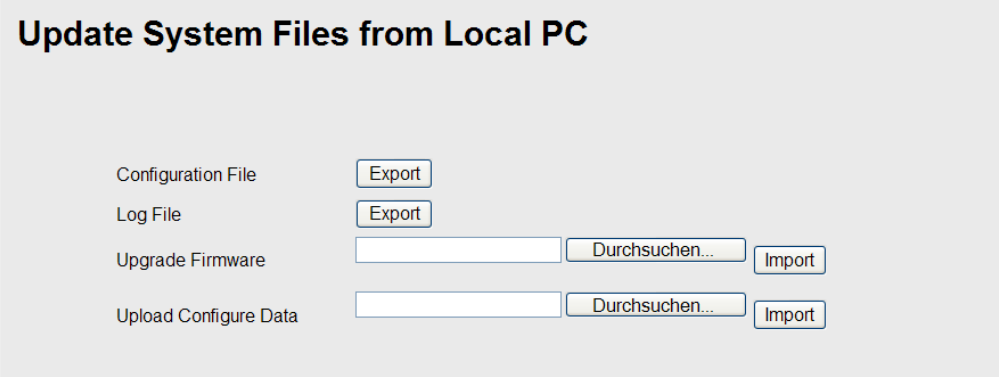
Log Files Path and Name

Setting	Description	Factory Default

Max. 40 Characters	The path and file name of the devices's log file	None

After setting up the desired path and file name, click **Activate** to save the setting, and then click **Download** to download the prepared file from the remote TFTP server, or click **Upload** to upload the desired file to the remote TFTP server.

System File Update: By Local Import/Export



Configuration File

To export the configuration file of this switch, click **Export** to save it to the local host.

Log File

To export the Log file of this switch, click **Export** and save it to the local host.

NOTE Some operating systems will open the configuration file and log file directly in the web page. In such cases, right click the "Export" button to save a file.

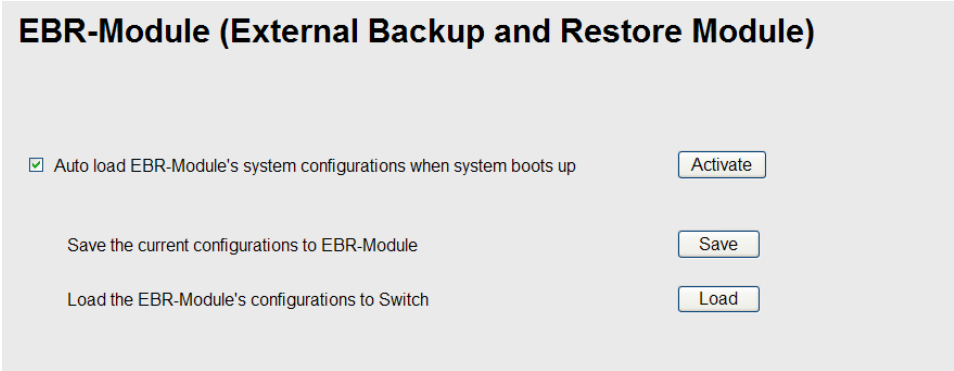
Upgrade Firmware

To import the firmware file of the device, click **Browse** to select the firmware file already saved on your computer. The upgrade procedure will proceed automatically after you click **Import**.

Upload Configuration Data

To import the configuration file of the device, click **Browse** to select the configuration file already saved on your computer. The upgrade procedure will proceed automatically after you click **Import**.

System File Update: By Backup Media


EBR-Module (External Backup and Restore Module)
Auto load EBR-Module's system configurations when system boots up
Activate
Save the current configurations to EBR-Module
Save
Load the EBR-Module's configurations to Switch
Load

Auto load system configurations when system boots up

Setting	Description	Factory Default
Enable	Enables Auto load system configurations when system boots up	Enable
Disable	Disables Auto load system configurations when system boots up	

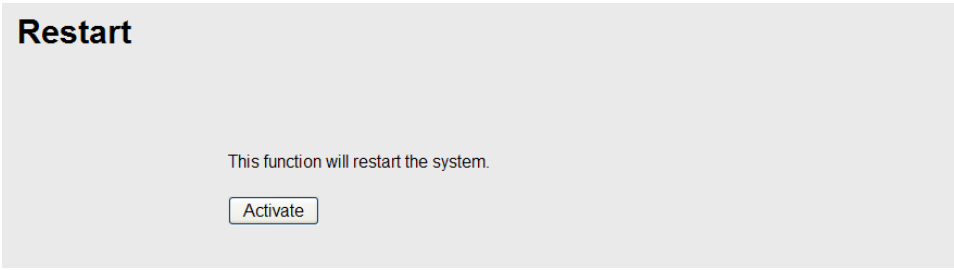
Save the current configurations to ABC

To export the current configuration file of the device, click on **Save** to save it to the ABC.

Load the ABC's configurations to the Switch

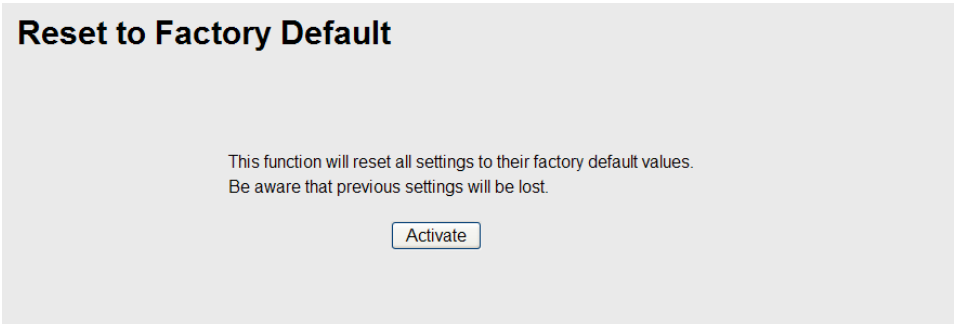
To import the configuration file of the device, click on **Load** to load it to the Switch.

Restart



This function is used to restart the Ethernet Switch.

Factory Default


Reset to Factory Default
This function will reset all settings to their factory default values.
Be aware that previous settings will be lost.
Activate

The Factory Default function is included to give users a quick way of restoring the IE-SW-VL08M's configuration settings to their factory default values. This function can be accessed from either the telnet/RS-232 Console, or Web Browser interface.

NOTE After activating the Factory Default function, you must use the default network settings to re-establish a web-browser or Telnet connection with your Weidmueller Switch.

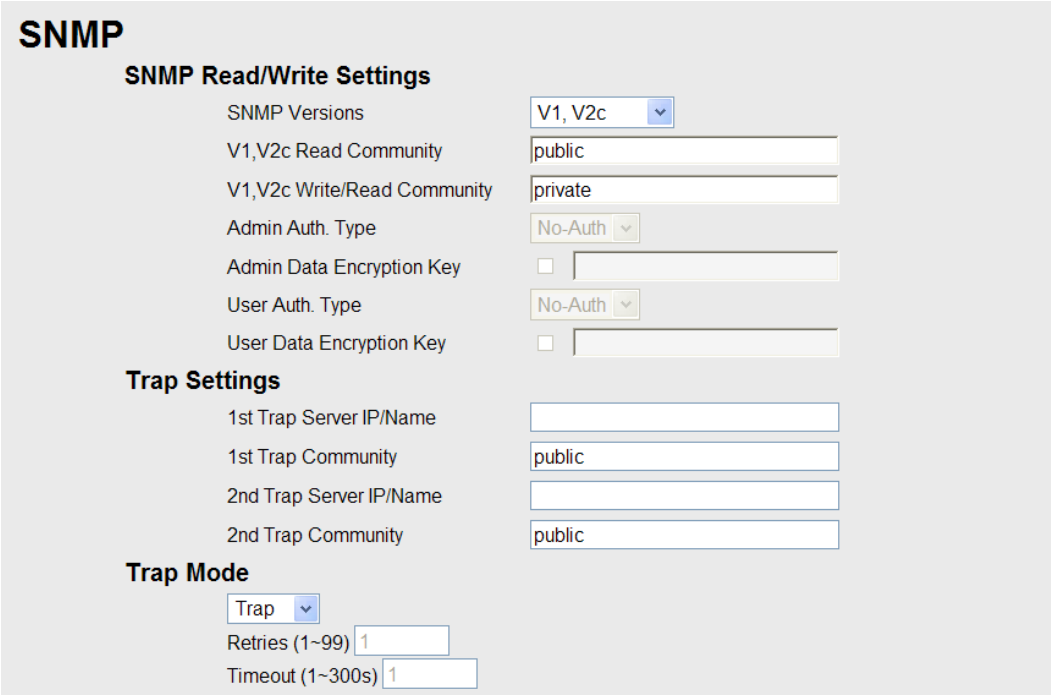
Configuring SNMP

Weidmueller Industrial Ethernet switches support SNMP protocol. The available versions are SNMP V1, SNMP V2c, and SNMP V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means SNMP servers access all objects with read-only or read/write permissions using the community string *public/private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

SNMP security modes and security levels supported by the device are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	Security Mode	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects
	MD5 or SHA	MD5 or SHA	No	Provides authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	MD5 or SHA	Data encryption key	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

The SNMP page can be configured. A more detailed explanation of each parameter follows:



SNMP Read/Write Settings

SNMP Versions

Setting	Description	Factory Default
V1, V2c, V3	Select SNMP protocol versions V1, V2c, V3 to manage the switch	V1, V2c
V1, V2c	Select SNMP protocol versions V1, V2c to manage the switch	
V3 only	Select only SNMP protocol version V3 to manage the switch	

V1, V2c Read Community

Setting	Description	Factory Default
V1, V2c Read Community	Use a community string match for authentication. This means that the SNMP agent accesses all objects with read-only permissions using the community string *public*.	public Maximum 30 characters

V1, V2c Write/Read Community

Setting	Description	Factory Default
V1, V2c Read/Write Community	Uses a community string match for authentication, which means that SNMP servers access all objects with read/write permissions using the community string *private*.	private Maximum 30 characters

For SNMP V3, there are two levels of privilege for different accounts to access the IE-SW-VL08M. **Admin** privilege allows access, and authorization to read and write the MIB file. **User** privilege only allows reading the MIB file, but does not authorize writing.

Admin Auth. Type *(for SNMP V1, V2c, V3, and V3 only)*

Setting	Description	Factory Default
No-Auth	Use admin account to access objects. No authentication	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

Admin Data Encryption Key *(for SNMP V1, V2c, V3, and V3 only)*

Setting	Description	Factory Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key	No
Disable	No data encryption	No

User Auth. Type *(for SNMP V1, V2c, V3 and V3 only)*

Setting	Description	Factory Default
No-Auth	Use the admin or user account to access objects. No authentication.	No
MD5-Auth	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No
SHA-Auth	Provide authentication based on the HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	No

User Data Encryption Key *(for SNMP V1, V2c, V3 and V3 only)*

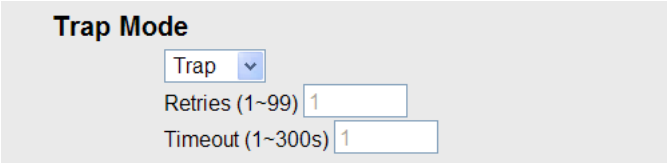
Setting	Description	Factory Default
Enable	8-character data encryption key is the minimum requirement for data encryption. Maximum 30-character encryption key.	No
Disable	No data encryption	No

Trap Settings

SNMP traps allow an SNMP agent to notify the NMS of a significant event. The IE-SW-VL08M supports two SNMP modes, **Trap** mode and **Inform** mode.

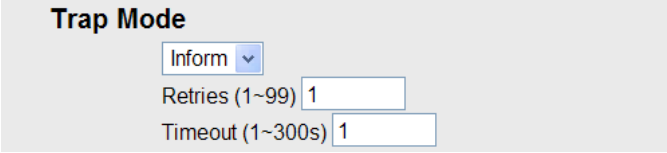
SNMP Trap Mode

In **Trap** mode, the SNMP agent sends an SNMPv1 trap PDU to the NMS. No acknowledgment is sent back from the NMS so the agent has no way of knowing if the trap reached the NMS.



SNMP Inform Mode

SNMPv2 provides an inform mechanism. When an inform message is sent from the SNMP agent to the NMS, the receiver sends a response to the sender acknowledging receipt of the event. This behavior is similar to that of the get and set requests. If the SNMP agent doesn't receive a response from the NMS for a period of time, the agent will resend the trap to the NMS agent. The maximum timeout time is 300 sec (default is 1 sec), and the maximum number of retries is 99 times (default is 1 time). When the SNMP agent receives acknowledgement from the NMS, it will stop resending the inform messages.



1st Trap Server IP/Name

Setting	Description	Factory Default
IP or Name	Enter the IP address or name of the 1st Trap Server used by your network.	None

1st Trap Community

Setting	Description	Factory Default
Character String	Use a community string match for authentication (maximum of 30 characters).	Public

2nd Trap Server IP/Name

Setting	Description	Factory Default
IP or Name	Enter the IP address or name of the 2nd Trap Server used by your network.	*None*

2nd Trap Community

Setting	Description	Factory Default
Character String	Use a community string match for authentication (maximum of 30 characters).	Public

Inform mode select

Setting	Description	Factory Default
Retries	Enter Inform Retry number	1
Time out	Enter Inform Timeout window	1

Private MIB information

Switch Object ID

Setting	Description	Factory Default
8691.7.6 8691.7.7	IE-SW-VL08M's enterprise value IE-SW-VL08M's enterprise value	Fixed

Note: This value cannot be changed.

Using Communication Redundancy

Setting up Communication Redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum.

The Communication Redundancy function allows the user to set up *redundant loops* in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable. For example, if the Industrial Ethernet switch is using a key communications component of a production line, several minutes of downtime could cause a big loss in production and revenue. Weidmueller Switches supports the following different protocols to support communication redundancy function:

→ **Rapid Spanning Tree/ Spanning Tree Protocol (IEEE 802.1W/1D),**

→ **Turbo Ring / Turbo Ring V2**

→ and **Turbo Chain**.

When configuring a redundant ring, all switches on the same ring must be configured to use the same redundancy protocol. You cannot mix the "Turbo Ring," "Turbo Ring V2," and STP/RSTP protocols on the same ring. The following table lists the key differences between each feature. Use this information to evaluate the benefits of each, and then determine which features are most suitable for your network.

	Turbo Ring V2	Turbo Ring	Turbo Chain	STP	RSTP
Topology	Ring	Ring	Chain	Ring, Mesh	Ring, Mesh
Recovery Time	< 20 ms	< 300 ms	< 20 ms	Up to 30 sec.	Up to 5 sec

NOTE All of Weidmueller's managed switches now support the three Turbo Ring protocols:

(1) **"Turbo Ring"** refers to the first version of redundant ring protocol, which has a recovery time of under 300 ms.
(2) **"Turbo Ring V2"** refers to the new generation Turbo Ring, which has a recovery time of under 20 ms.

(3) "**Turbo Chain**" is a new protocol with unlimited flexibly to allow you to construct any type of redundant network topology. The recovery time is under 20 ms.

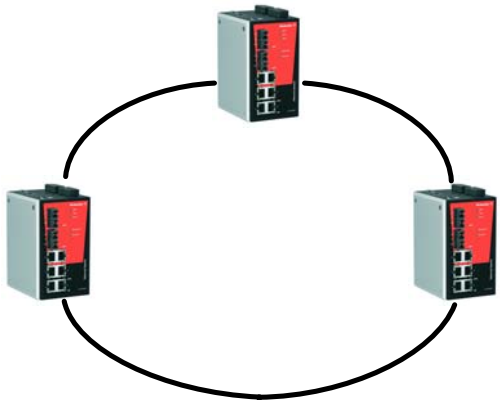
In this manual, we use the terminology ***"Turbo Ring" ring*** and ***"Turbo Ring V2" ring*** to differentiate between rings configured for one or the other of these protocols.

The Turbo Ring Concept

The Turbo Ring protocol was developed to optimize communication redundancy and achieve a faster recovery time on the network.

The Turbo Ring and Turbo Ring V2 protocols identify one switch as the ***master*** of the network, and then automatically block packets from traveling through any of the network's redundant loops. In the event that one branch of the ring gets disconnected from the rest of the network, the protocol automatically readjusts the ring so that the part of the network that was disconnected can reestablish contact with the rest of the network.

Initial setup of a "Turbo Ring" or "Turbo Ring V2" ring



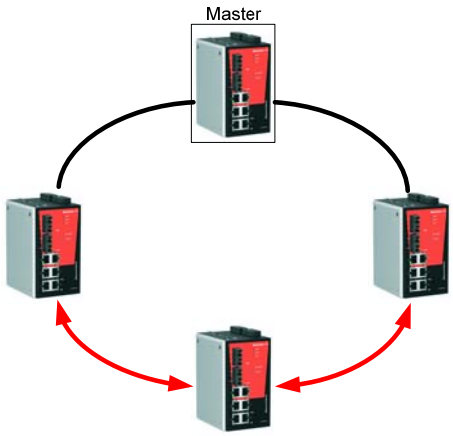
1. For each switch in the ring, select any two ports as the redundant ports.
2. Connect redundant ports on neighboring switches to form the redundant ring.

The user does not need to configure any of the switches as the master to use Turbo Ring or Turbo Ring V2. If none of the switches in the ring is configured as the master, then the protocol will automatically assign master status to one of the switches. In fact, the master is only used to identify which segment in the redundant ring acts as the backup path. In the following subsections, we explain how the redundant path is selected for rings configured for Turbo Ring, and Turbo Ring V2.

Determining the Redundant Path of a "Turbo Ring" Ring

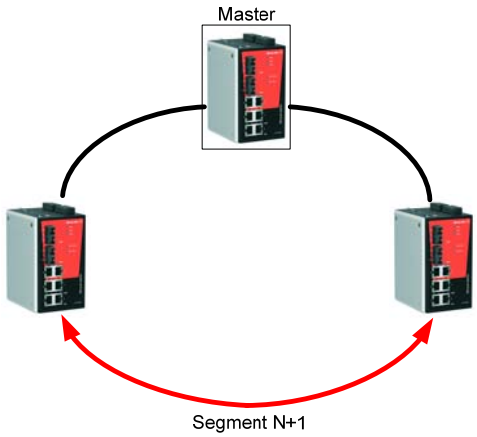
In this case, the redundant segment (i.e., the segment that will be blocked during normal operation) is determined by the number of switch units that make up the ring, and where the ring master is located.

"Turbo Ring" rings with an even number of Weidmueller switch units



If there are 2N IE-SW units (an even number) in the "Turbo Ring" ring, then the backup segment is one of the two segments connected to the (N+1) st IE-SW (i.e., the IE-SW unit directly opposite the master).

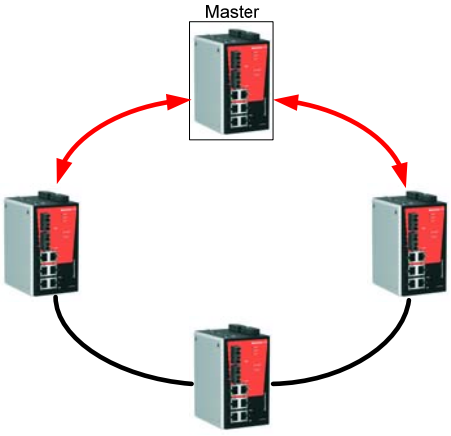
"Turbo Ring" rings with an odd number of Weidmueller switch units



If there are 2N+1 IE-SW units (an odd number) in the "Turbo Ring" ring, with IE-SW units and segments labeled counterclockwise, then segment N+1 will serve as the backup path.

For the example shown here, N=1, so that N+1=2.

Determining the Redundant Path of a "Turbo Ring V2" Ring



For a "Turbo Ring V2" ring, the backup segment is the segment connected to the 2nd redundant port on the master.

See **Configuring "Turbo Ring V2"** in the **Configuring "Turbo Ring" and "Turbo Ring V2"** section below.

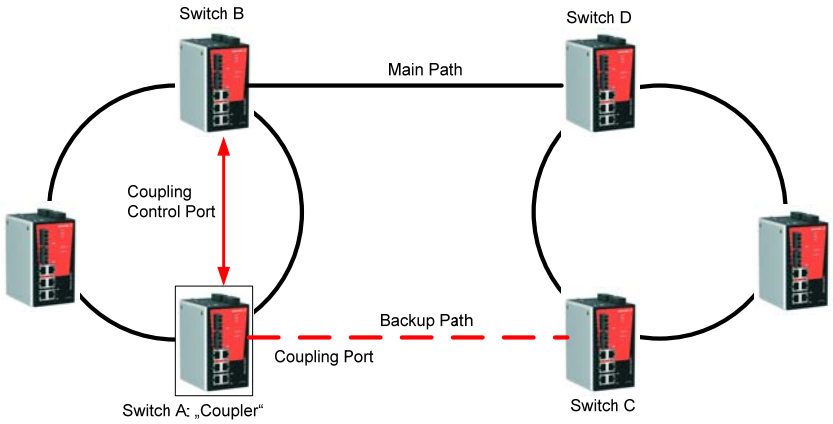
Ring Coupling Configuration

For some systems, it may not be convenient to connect all devices in the system to create one BIG redundant ring, since some devices could be located in a remote area. For these systems, "Ring Coupling" can be used to separate the devices into different smaller redundant rings, but in such a way that they can still communicate with each other.

ATTENTION

In a VLAN environment, the user must set "Redundant Port," "Coupling Port," and "Coupling Control Port" to join all VLANs, since these ports act as the "backbone" to transmit all packets of different VLANs to different IE-SW-VL08M units.

Ring Coupling for a "Turbo Ring" Ring

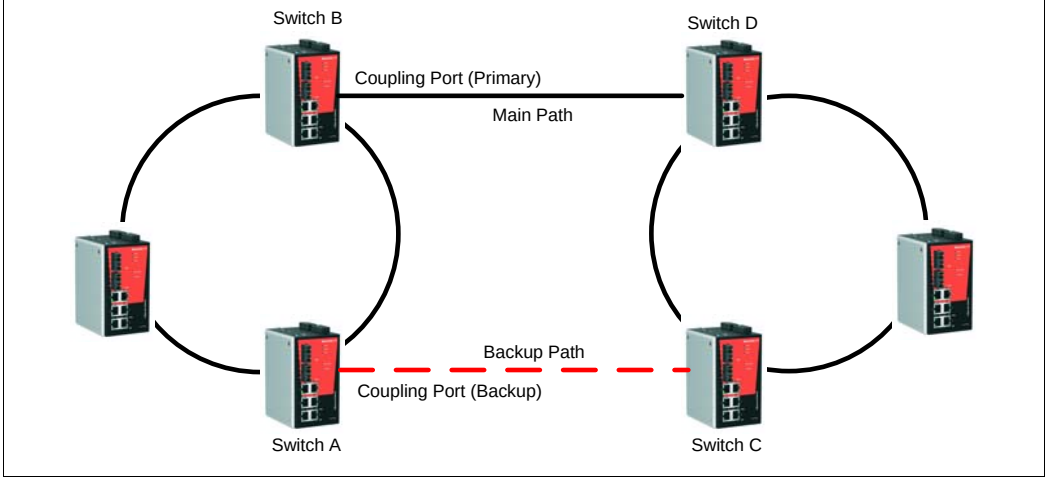


To configure the Ring Coupling function for a "Turbo Ring" ring, select two switch units (e.g., Switch A and B in the above figure) in the ring, and another two switch units in the adjacent ring (e.g., Switch C and D).

Decide which two ports in each switch are appropriate to be used as coupling ports, and then link them together. Next, assign one switch (e.g., Switch A) to be the "coupler," and connect the coupler's coupling control port with Switch B (for this example).

The coupler switch (i.e., Switch A) will monitor switch B through the coupling control port to determine whether or not the coupling port's backup path should be recovered.

Ring Coupling for a "Turbo Ring V2" Ring



Note that the ring coupling settings for a "Turbo Ring V2" ring are different from a "Turbo Ring" ring. For Turbo Ring V2, Ring Coupling is enabled by configuring the "Coupling Port (Primary)" on Switch B, and the "Coupling Port (Backup)" on Switch A only. You do not need to set up a coupling control port, so that a "Turbo Ring V2" ring does not use a coupling control line.

The "Coupling Port (Backup)" on Switch A is used for the backup path, and connects directly to an extra network port on Switch C. The "Coupling Port (Primary)" on Switch B monitors the status of the main path, and connects directly to an extra network port on Switch D. With ring coupling established, Switch A can activate the backup path as soon as it detects a problem with the main path.

ATTENTION

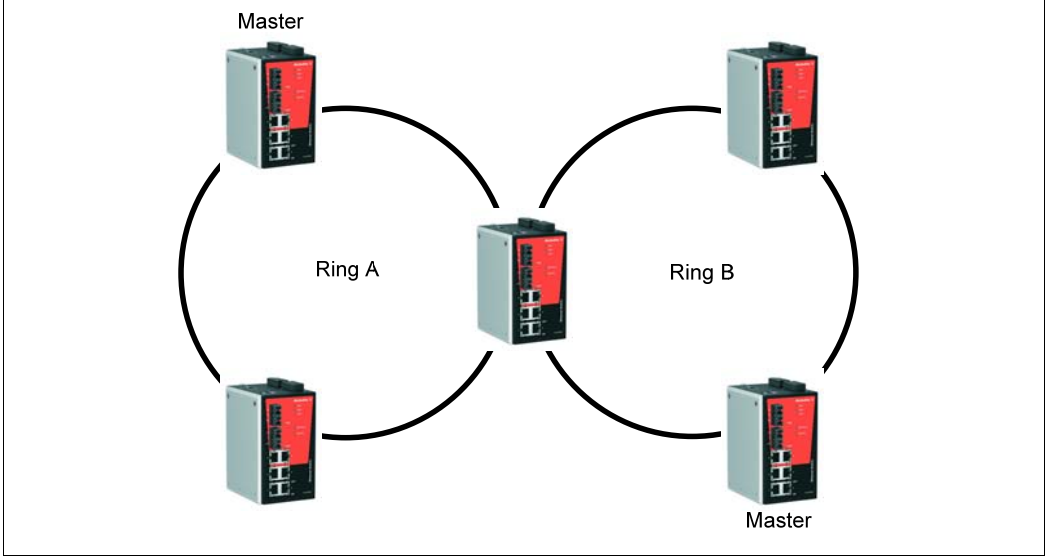
Ring Coupling only needs to be enabled on one of the switches serving as the Ring Coupler. The Coupler must designate different ports as the two Turbo Ring ports and the coupling port.

NOTE You do not need to use the same IE-SW-VL08M unit for both Ring Coupling and Ring Master.

Dual-Ring Configuration (applies only to "Turbo Ring V2")

The "dual-ring" option provides another ring coupling configuration, in which two adjacent rings share one switch. This type of configuration is ideal for applications that have inherent cabling difficulties.

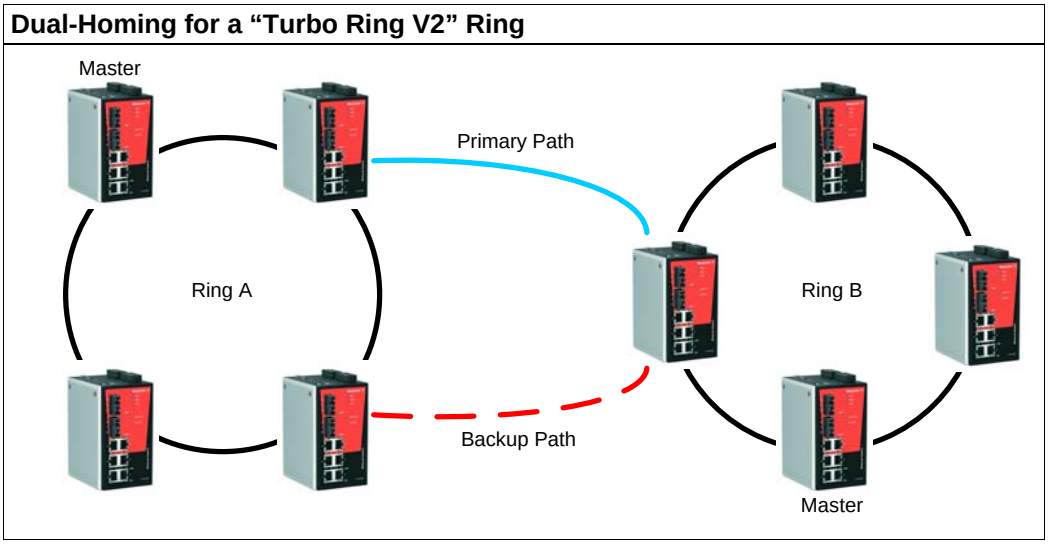
Dual-Ring for a "Turbo Ring V2" Ring



Dual-Homing Configuration (applies only to "Turbo Ring V2")

The "dual-homing" option uses a single Ethernet switch to connect two networks. The primary path is the operating connection, and the backup path is a back-up connection that is activated in the event that the primary path connection fails.

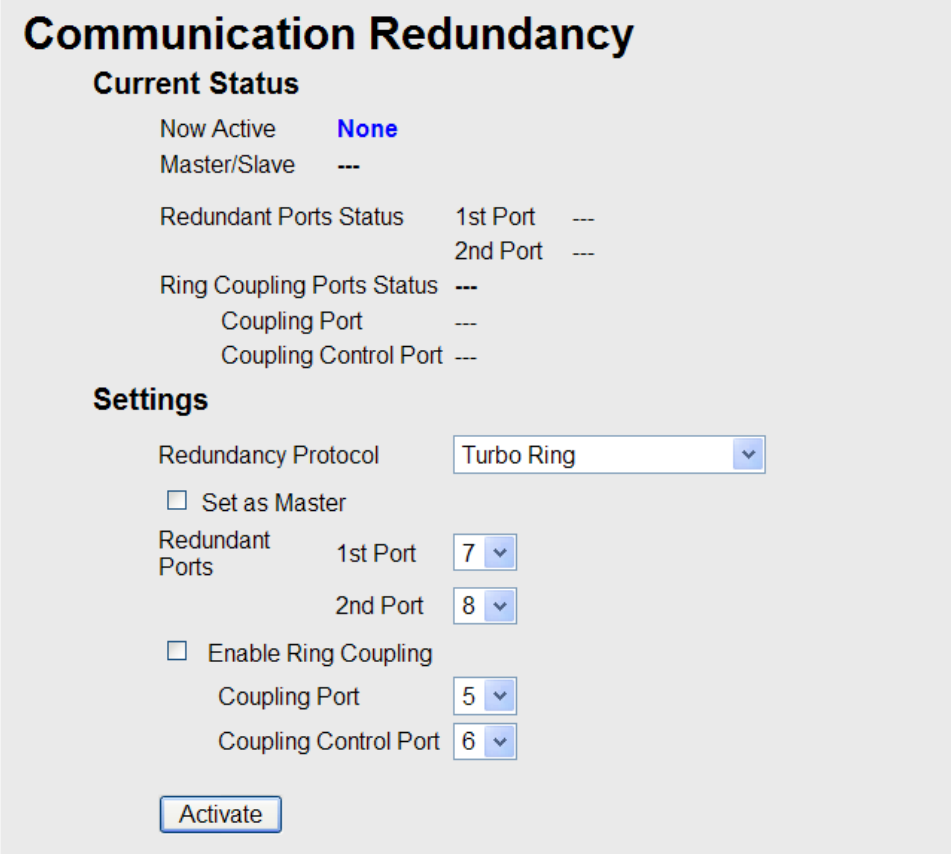
Dual-Homing for a "Turbo Ring V2" Ring



Configuring "Turbo Ring" and "Turbo Ring V2"

Use the **Communication Redundancy** page to configure select "Turbo Ring" or "Turbo Chain" or "Turbo Ring V2." Note that configuration pages for these two protocols are different.

Configuring "Turbo Ring"



Explanation of "Current Status" Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, or **none**.

Master/Slave

Indicates whether or not this device is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the Weidmueller Switch units in the ring. The master is only used to determine which segment serves as the backup path.

Redundant Ports Status (1st Port, 2nd Port)

Ring Coupling Ports Status (Coupling Port, Coupling Control Port)

The "Ports Status" indicators show ***Forwarding*** for normal transmission, ***Blocking*** if this port is connected to a backup path and the path is blocked, and ***Link down*** if there is no connection.

Explanation of "Settings" Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Set as Master

Setting	Description	Factory Default
Enabled	Select this Switch as Master	Not checked
Disabled	Do not select this Switch as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the Switch to be one of the redundant ports.	Port 4 Port 7
2nd Port	Select any port of the Switch to be one of the redundant ports.	Port 5 Port 8

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this Switch as Coupler	Not checked
Disable	Do not select this Switch as Coupler	

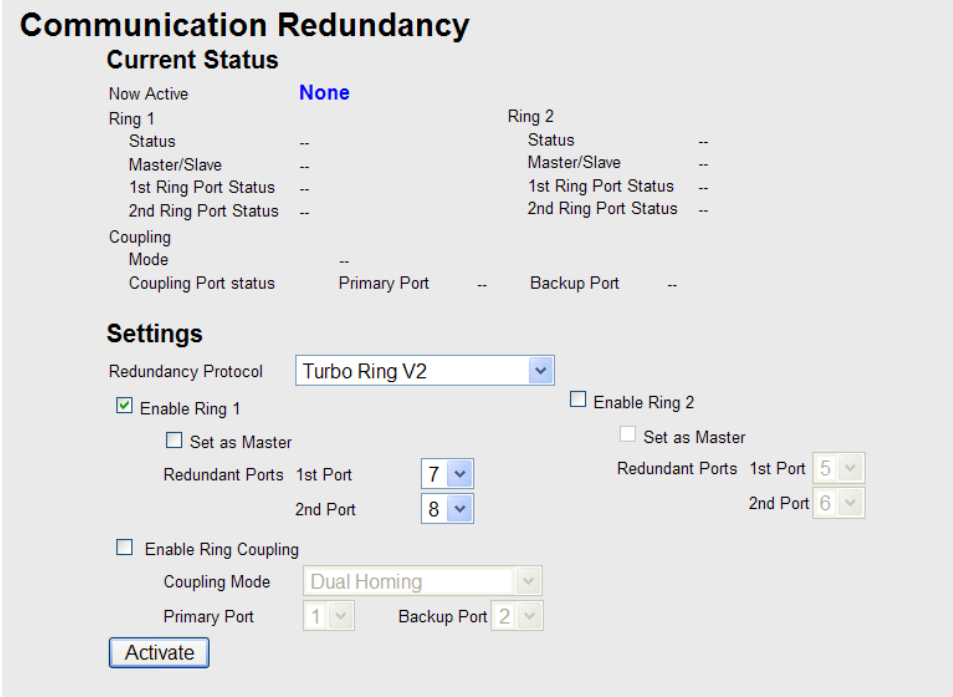
Coupling Port

Setting	Description	Factory Default
Coupling Port	Select any port of the Switch to be the coupling port	Port 2 Port 5

Coupling Control Port

Setting	Description	Factory Default
Coupling Control Port	Select any port to be the coupling control port	Port 3 Port 6

Configuring "Turbo Ring V2"



NOTE When using the Dual-Ring architecture, users must configure settings for both Ring 1 and Ring 2. In this case, the status of both rings will appear under "Current Status."

Explanation of "Current Status" Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **Turbo Chain**, **RSTP**, or **none**.

Ring 1/2—Status

Shows **Healthy** if the ring is operating normally, and shows **Break** if the ring's backup link is active.

Ring 1/2—Master/Slave

Indicates whether or not this switch is the Master of the Turbo Ring. (This field appears only when selected to operate in Turbo Ring or Turbo Ring V2 mode.)

NOTE The user does not need to set the master to use Turbo Ring. If no master is set, the Turbo Ring protocol will assign master status to one of the switch units in the ring. The master is only used to determine which segment serves as the backup path.

Ring 1/2—1st Ring Port Status

Ring 1/2—2nd Ring Port Status

The "Ports Status" indicators show ***Forwarding*** for normal transmission, ***Blocking*** if this port is connected to a backup path and the path is blocked, and ***Link down*** if there is no connection.

Coupling—Mode

Indicates either **None**, **Dual Homing**, or **Ring Coupling**.

Coupling—Coupling Port status

Indicates either **Primary**, or **Backup**.

Explanation of "Settings" Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page.	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Enable Ring 1

Setting	Description	Factory Default
Enabled	Enable the Ring 1 settings	Not checked
Disabled	Disable the Ring 1 settings	

Enable Ring 2*

Setting	Description	Factory Default
Enabled	Enable the Ring 2 settings	Not checked
Disabled	Disable the Ring 2 settings	

***You should enable both Ring 1 and Ring 2 when using the Dual-Ring architecture.**

Set as Master

Setting	Description	Factory Default
Enabled	Select this switch as Master	Not checked
Disabled	Do not select this switch as Master	

Redundant Ports

Setting	Description	Factory Default
1st Port	Select any port of the switch to be one of the redundant ports.	Port 4 Port 7
2nd Port	Select any port of the switch to be one of the redundant ports.	Port 5 Port 8

Enable Ring Coupling

Setting	Description	Factory Default
Enable	Select this switch as Coupler	Not checked
Disable	Do not select this switch as Coupler	

Coupling Mode

Setting	Description	Factory Default
Dual Homing	Select this item to change to the Dual Homing configuration page	Primary Port: Port 5 Backup Port: Port 6 Primary Port: Port 2 Backup Port: Port 3
Ring Coupling (backup)	Select this item to change to the Ring Coupling (backup) configuration page	Port 5 Port 2
Ring Coupling (primary)	Select this item to change to the Ring Coupling (primary) configuration page	Port 5 Port 2

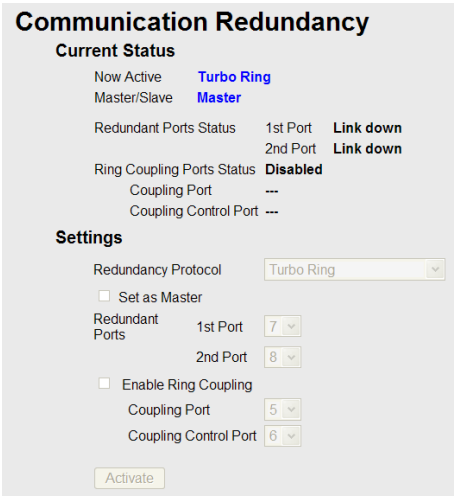
Primary/Backup Port

Setting	Description	Factory Default
Primary Port	Select any port of the switch to be the primary port.	Port 2 Port 5
Backup Port	Select any port of the switch to be the backup port.	Port 3 Port 6

NOTE

The Turbo Ring DIP Switches located on the IE-SW-VL08M's outer casing can be used to configure the devices's Turbo Ring protocols. (For details on how to do this, refer to "Configuring Basic Settings—Turbo Ring DIP Switch" section in this manual.)

If you use the web interface, console interface, or Telnet interface to enable the Turbo Ring DIP Switches, and then set DIP Switch 4 on the switch's outer casing to the "ON" position, you will not be able to use the web interface, console interface, or Telnet interface to change the status of the DIP Switch. In this case, the **Communication Redundancy** settings will be "grayed out" in the web browser as shown in the following figure:

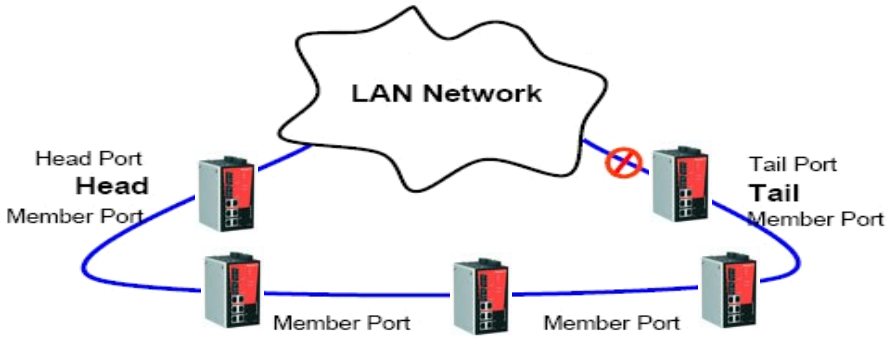


The Turbo Chain Concept

The Turbo Chain is an advanced software-technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the "chain" concept, you first connect the Ethernet switches in a chain and then simply link the two ends of the chain to an Ethernet network, as illustrated in the following figure.

Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses a multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.

Setting Up Turbo Chain

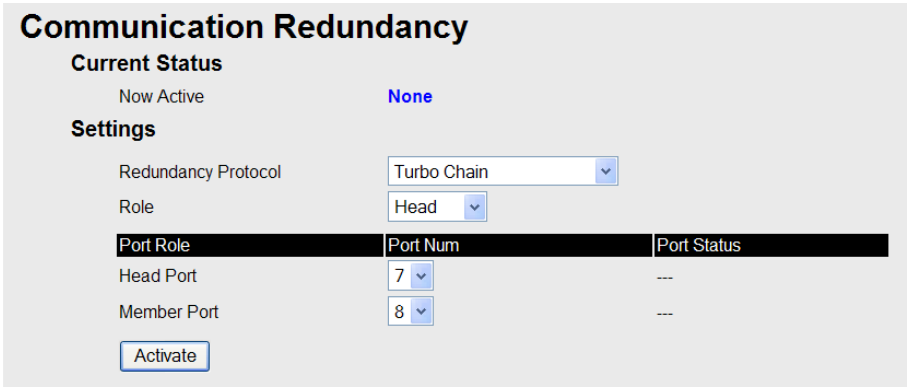


1. Select the Head switch, Tail switch, and Member switches.
2. Configure one port as the Head port and one port as the Member port in the Head switch, configure one port as the Tail port and one port as the Member port in the Tail switch, and configure two ports as Member ports in each of the Member switches.
3. Connect the Head switch, Tail switch, and Member switches as shown in the diagram.

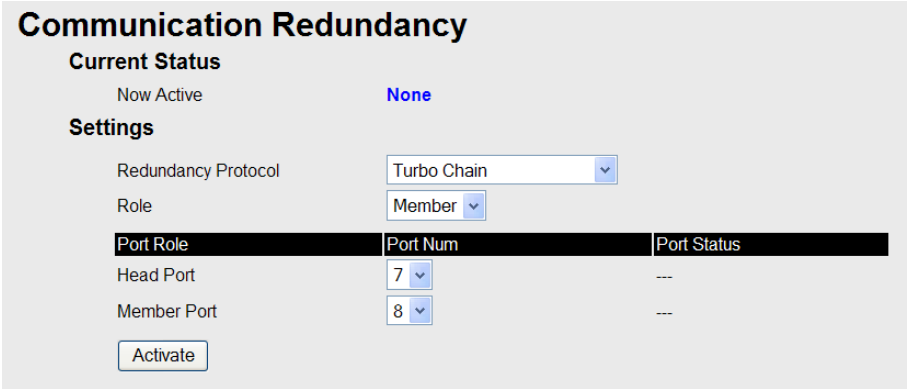
The path connecting to the Head port is the main path, and the path connecting to the Tail port is the backup path of the Turbo Chain. Under normal conditions, packets are transmitted through the Head Port to the LAN Network. If any Turbo Chain path is disconnected, the Tail Port will be activated to continue packet transmission.

Configuring "Turbo Chain"

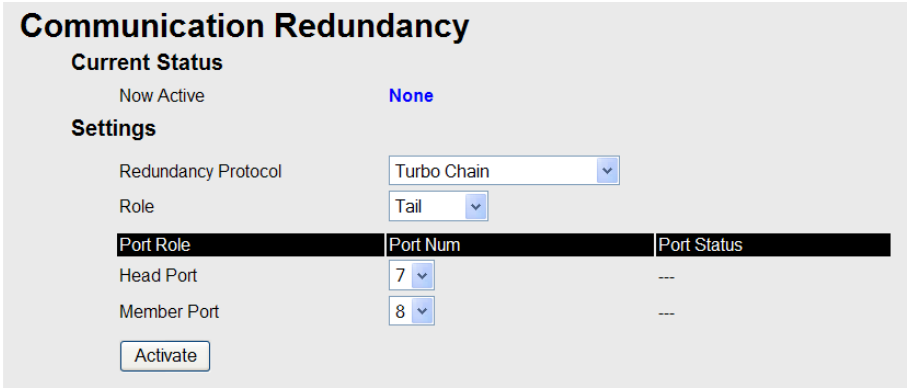
Head Switch Configuration



Member Switch Configuration



Tail Switch Configuration



Explanation of "Current Status" Items

Now Active

Shows which communication protocol is in use: **Turbo Ring**, **Turbo Ring V2**, **RSTP**, **Turbo Chain** or **None**.

The "Ports Status" indicators show ***Forwarding*** for normal transmission, ***Blocked*** if this port is

connected to the Tail port as a backup path and the path is blocked, and ***Link down*** if there is no connection.

Explanation of "Settings" Items

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Role

Setting	Description	Factory Default
Head	Select this switch as Head Switch	Member
Member	Select this switch as Member Switch	
Tail	Select this switch as Tail Switch	

Head Role

Setting	Description	Factory Default
Head Port	Select any port of the switch to be the head port.	Port 4 Port 7
Member Port	Select any port of the switch to be the member port.	Port 5 Port 8

Member Role

Setting	Description	Factory Default
1st Member port	Select any port of the switch to be the 1st member port	Port 4 Port 7
2nd Member port	Select any port of the switch to be the 2nd member port	Port 5 Port 8

Tail Role

Setting	Description	Factory Default
Tail Port	Select any port of the switch to be the tail port.	Port 4 Port 7
Member Port	Select any port of the switch to be the member port.	Port 5 Port 8

The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. Weidmueller Switch's STP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every switch connected to your network.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE Std 802.1w-2001. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:
  - Defaults to sending 802.1D style BPDUs if packets with this format are received.
  - STP (802.1D) and RSTP (802.1w) can operate on different ports of the same switch. This feature is particularly helpful when switch ports are connected to older equipment, such as legacy switches.

RSTP provides essentially the same functionality as STP. To see how the two systems differ, see the *Differences between RSTP and STP* section in this chapter.

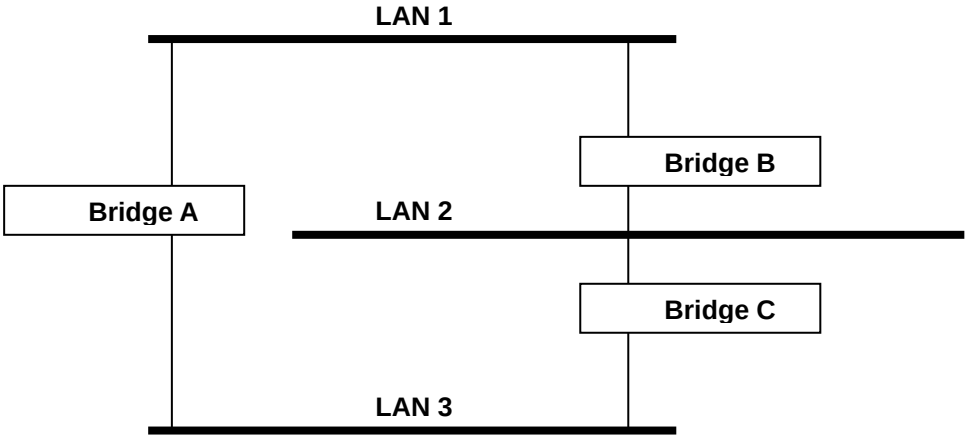
NOTE The STP protocol is part of the IEEE Std 802.1D, 1998 Edition bridge specification. The following explanation uses bridge instead of switch.

What is STP?

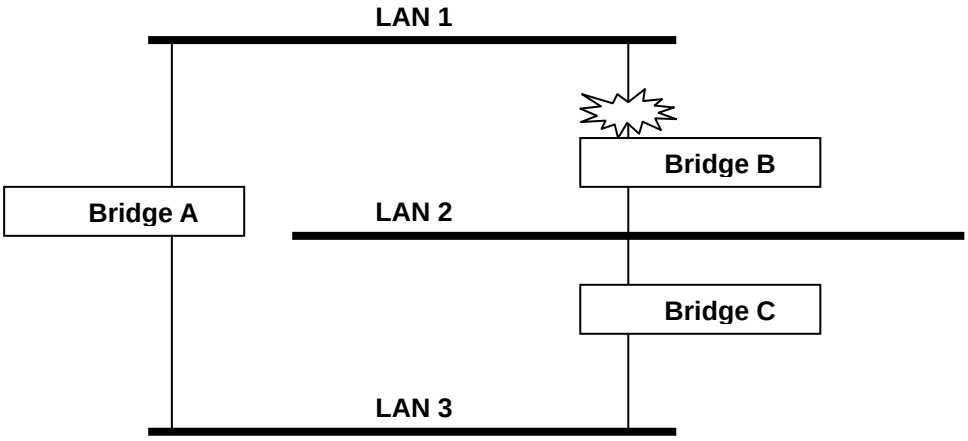
STP (802.1D) is a bridge-based system that is used to implement parallel paths for network traffic. STP uses a loop-detection process to:

- Locate and then disable less efficient paths (i.e., paths that have a lower bandwidth).
- Enable one of the less efficient paths if the most efficient path fails.

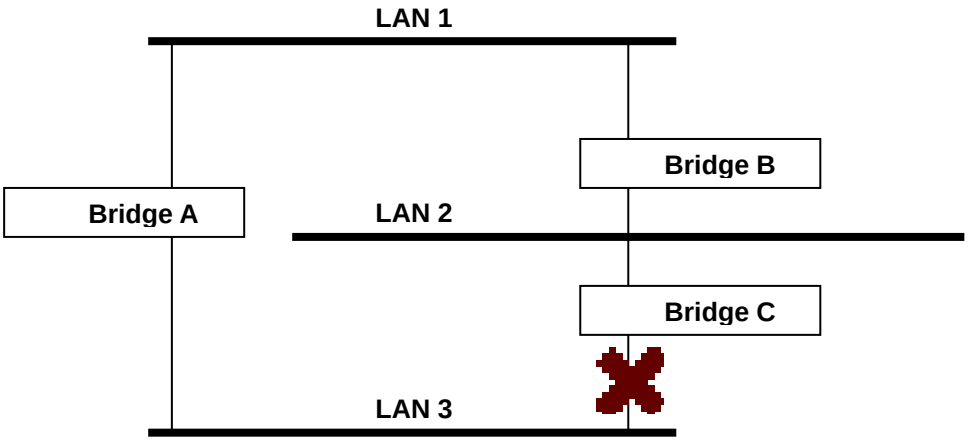
The figure below shows a network made up of three LANs separated by three bridges. Each segment uses at most two paths to communicate with the other segments. Since this configuration can give rise to loops, the network will overload if STP is NOT enabled.



If STP is enabled, it will detect duplicate paths and prevent, or *block*, one of them from forwarding traffic. In the following example, STP determines that traffic from LAN segment 2 to LAN segment 1 should flow through Bridges C and A as this path has a greater bandwidth and is therefore more efficient.



What happens if a link failure is detected? As shown in next figure, the STP process reconfigures the network so that traffic from LAN segment 2 flows through Bridge B.



STP determines which path between each bridged segment is most efficient, and then assigns a specific reference point on the network. When the most efficient path has been identified, the other paths are blocked. In the previous 3 figures, STP first determined that the path through Bridge C was the most efficient, and as a result, blocked the path through Bridge B. After the failure of Bridge C, STP re-evaluated the situation and opened the path through Bridge B.

How STP Works

When enabled, STP determines the most appropriate path for traffic through a network. The way it does this is outlined in the following sections.

STP Requirements

Before STP can configure the network, the system must satisfy the following requirements:

- Communication between all the bridges. This communication is carried out using Bridge Protocol Data Units (BPDUs), which are transmitted in packets with a known multicast address.
- Each bridge must have a Bridge Identifier that specifies which bridge acts as the central reference point, or Root Bridge, for the STP system—bridges with a lower Bridge Identifier are more likely to be designated as the Root Bridge. The Bridge Identifier is calculated using the MAC address of the bridge and a priority defined for the bridge. The default priority of IE-SW-VL08M is 32768.
- Each port has a cost that specifies the efficiency of each link. The efficieny cost is usually

determined by the bandwidth of the link, with less efficient links assigned a higher cost. The following table shows the default port costs for a switch:

Port Speed	Path Cost 802.1D, 1998 Edition	Path Cost 802.1w-2001
10 Mbps	100	2,000,000
100 Mbps	19	200,000
1000 Mbps	4	20,000

STP Calculation

The first step of the STP process is to perform calculations. During this stage, each bridge on the network transmits BPDUs. The following items will be calculated:

- The bridge that should be the Root Bridge. The Root Bridge is the central reference point from which the network is configured.
- The Root Path Costs for each bridge. This is the cost of the paths from each bridge to the Root Bridge.
- The identity of each bridge's Root Port. The Root Port is the port on the bridge that connects to the Root Bridge via the most efficient path; in other words, the port connected to the Root Bridge via the path with the lowest Root Path Cost. The Root Bridge, however, does not have a Root Port.
- The identity of the Designated Bridge for each LAN segment. The Designated Bridge is the bridge with the lowest Root Path Cost from that segment. If several bridges have the same Root Path Cost, the one with the lowest Bridge Identifier becomes the Designated Bridge. Traffic transmitted in the direction of the Root Bridge will flow through the Designated Bridge. The port on this bridge that connects to the segment is called the Designated Bridge Port.

STP Configuration

After all the bridges on the network agree on the identity of the Root Bridge, and all other relevant parameters have been established, each bridge is configured to forward traffic only between its Root Port and the Designated Bridge Ports for the respective network segments. All other ports are blocked, which means that they will not be allowed to receive or forward traffic.

STP Reconfiguration

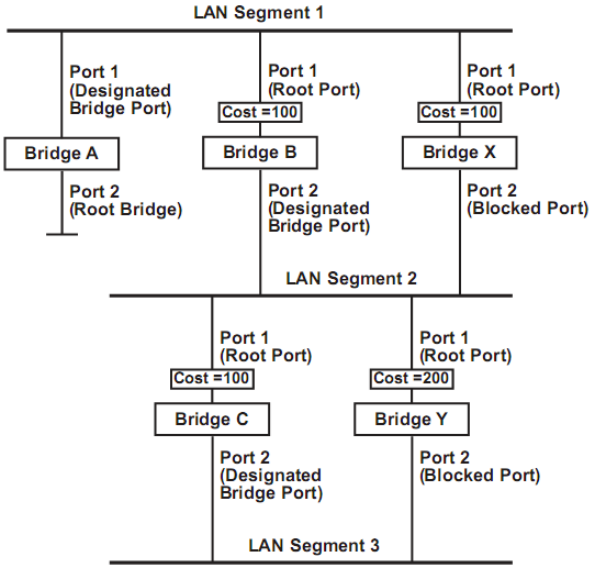
Once the network topology has stabilized, each bridge listens for Hello BPDUs transmitted from the Root Bridge at regular intervals. If a bridge does not receive a Hello BPDU after a certain interval (the Max Age time), the bridge assumes that the Root Bridge, or a link between itself and the Root Bridge, has gone down. This will trigger the bridge to reconfigure the network to account for the change. If you have configured an SNMP trap destination, when the topology of your network changes, the first bridge to detect the change sends out an SNMP trap.

Differences between RSTP and STP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

STP Example

The LAN shown below has three segments, with adjacent segments connected using two possible links. The various STP factors, such as Cost, Root Port, Designated Bridge Port, and Blocked Port are shown in the figure.



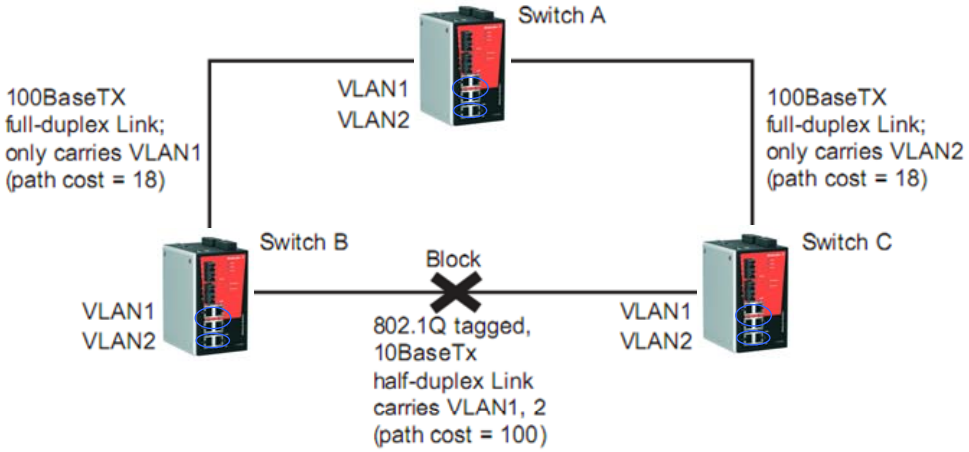
- Bridge A has been selected as the Root Bridge, since it was determined to have the lowest Bridge Identifier on the network.
- Since Bridge A is the Root Bridge, it is also the Designated Bridge for LAN segment 1. Port 1 on Bridge A is selected as the Designated Bridge Port for LAN Segment 1.
- Ports 1 of Bridges B, C, X, and Y are all Root Ports since they are nearest to the Root Bridge, and therefore have the most efficient path.

- Bridges B and X offer the same Root Path Cost for LAN segment 2. However, Bridge B was selected as the Designated Bridge for that segment since it has a lower Bridge Identifier. Port 2 on Bridge B is selected as the Designated Bridge Port for LAN Segment 2.
- Bridge C is the Designated Bridge for LAN segment 3, because it has the lowest Root Path Cost for LAN Segment 3:
  - The route through Bridges C and B costs 200 (C to B=100, B to A=100)
  - The route through Bridges Y and B costs 300 (Y to B=200, B to A=100)
- The Designated Bridge Port for LAN Segment 3 is Port 2 on Bridge C.

Using STP on a Network with Multiple VLANs

IEEE Std 802.1D, 1998 Edition, does not take into account VLANs when calculating STP information—the calculations depend only on the physical connections. Consequently, some network configurations will result in VLANs being subdivided into a number of isolated sections by the STP system. You must ensure that every VLAN configuration on your network takes into account the expected STP topology and alternative topologies that may result from link failures. The following figure shows an example of a network that contains VLANs 1 and 2. The VLANs are connected using the 802.1Q-tagged link between Switch B and Switch C. By default, this link has a port cost of 100 and is automatically blocked because the other Switch-to-Switch connections have a

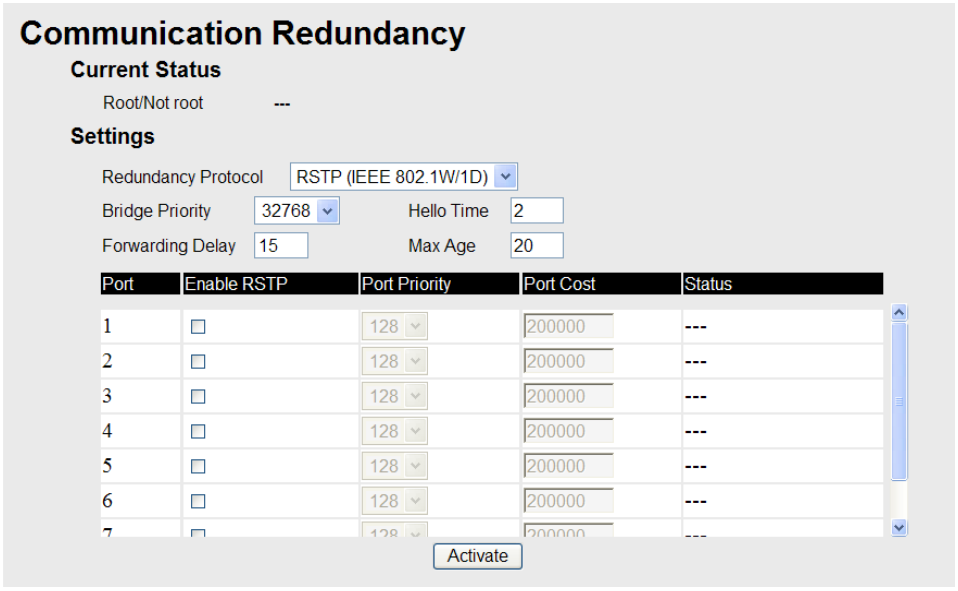
port cost of 36 (18+18). This means that both VLANs are now subdivided—VLAN 1 on Switch units A and B cannot communicate with VLAN 1 on Switch C, and VLAN 2 on Switch units A and C cannot communicate with VLAN 2 on Switch B.



To avoid subdividing VLANs, all inter-switch connections should be made members of all available 802.1Q VLANs. This will ensure connectivity at all times. For example, the connections between Switches A and B, and between Switches A and C should be 802.1Q tagged and carrying VLANs 1 and 2 to ensure connectivity.

Configuring STP/RSTP

The following figures indicate the Spanning Tree Protocol parameters that can be configured. A more detailed explanation of each parameter is given below the figure. (NOTE: The user interface for IE-SW-VL08M shows 8 ports.)



At the top of this page, the user can check the ***Current Status*** of this function. For RSTP, you will see:

Now Active:
This shows the communication protocol being used—Turbo Ring, RSTP, or none.

Root/Not Root
This is displayed only when RSTP is selected as the mode of operation. It indicates whether or not this device is the Root of the Spanning Tree (the root is determined automatically).

At the lower portion of this page, the user can configure the ***Settings*** of this function. For RSTP, you can configure:

Redundancy Protocol

Setting	Description	Factory Default
Turbo Ring	Select this item to change to the Turbo Ring configuration page.	None
Turbo Ring V2	Select this item to change to the Turbo Ring V2 configuration page.	
Turbo Chain	Select this item to change to the Turbo Chain configuration page	
RSTP (IEEE 802.1W/1D)	Select this item to change to the RSTP configuration page.	
None	Ring redundancy is not active	

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this device's bridge priority by selecting a lower number. A device with a higher bridge priority has a greater chance of being established as the root of the Spanning Tree topology.	32768

Forwarding Delay

Setting	Description	Factory Default
Numerical value input by user	The amount of time this device waits before checking to see if it should change to a different state.	15 (sec.)

Hello time (sec.)

Setting	Description	Factory Default
Numerical value input by user	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. The "hello time" is the amount of time the root waits between sending hello messages.	2

Max. Age (sec.)

Setting	Description	Factory Default
Numerical value input by user	If this device is not the root, and it has not received a hello message from the root in an amount of time equal to ***Max. Age***, then this device will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20

Enable STP per Port

Setting	Description	Factory Default
Enable/Disable	Select to enable the port as a node on the Spanning Tree topology.	Disabled

NOTE We suggest not enabling the Spanning Tree Protocol once the port is connected to a device (PLC, RTU, etc.) as opposed to network equipment. The reason is that it will cause unnecessary negotiation.

Port Priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by entering a lower number.	128

Port Cost

Setting	Description	Factory Default
Numerical value input by user	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology.	200000

Port Status

This indicates the current Spanning Tree status of this port. The status values are ***Forwarding*** for normal transmission, and ***Blocking*** to block transmission.

Configuration Limits of RSTP/STP

The Spanning Tree Algorithm places limits on three of the configuration items previously described:

[Eq. 1]: 1 sec ≦ Hello Time ≦ 10 sec

[Eq. 2]: 6 sec ≦ Max. Age ≦ 40 sec

[Eq. 3]: 4 sec ≦ Forwarding Delay ≦ 30 sec

These three variables are further restricted by the following two inequalities:

[Eq. 4]: 2 * (Hello Time + 1 sec) ≦ Max. Age ≦ 2 * (Forwarding Delay – 1 sec)

The switch's firmware will alert you immediately if any of these restrictions are violated. For example, setting

Hello Time = 5 sec, Max. Age = 20 sec, and Forwarding Delay = 4 sec does not violate Eqs. 1 through 3, but does violate Eq. 4, since in this case,

2 * (Hello Time + 1 sec) = 12 sec, and 2 * (Forwarding Delay – 1 sec) = 6 sec.

You can remedy the situation in a multitude of ways. One solution is simply to increase the Forwarding Delay to at least 11 sec.

HINT: Take the following steps to avoid guessing:

Step 1: Assign a value to ***Hello Time*** and then calculate the left most part of Eq. 4 to get the lower limit of ***Max. Age***.

Step 2: Assign a value to ***Forwarding Delay*** and then calculate the right most part of Eq. 4 to get the upper limit for ***Max. Age***.

Step 3: Assign a value to ***Forwarding Delay*** that satisfies the conditions in Eq. 3 and Eq. 4.

Using Traffic Prioritization

The DS's traffic prioritization capability provides Quality of Service (QoS) to your network by making data delivery more reliable. You can prioritize traffic on your network to ensure that high priority data is transmitted with minimum delay. Traffic can be controlled by a set of rules to obtain the required Quality of Service for your network. The rules define different types of traffic and specify how each type should be treated as it passes through the switch. The device can inspect both IEEE 802.1p/1Q layer 2 QoS tags, and even layer 3 TOS information to provide consistent classification of the entire network. The switch's QoS capability improves the performance and determinism of industrial networks for mission critical applications.

The Traffic Prioritization Concept

What is Traffic Prioritization?

Traffic prioritization allows you to prioritize data so that time-sensitive and system-critical data can be transferred smoothly and with minimal delay over a network. The benefits of using traffic prioritization are:

- Improve network performance by controlling a wide variety of traffic and managing congestion.
- Assign priorities to different categories of traffic. For example, set higher priorities for time-critical or business-critical applications.
- Provide predictable throughput for multimedia applications, such as video conferencing or voice over IP, and minimize traffic delay and jitter.
- Improve network performance as the amount of traffic grows. This will save cost by reducing the need to keep adding bandwidth to the network.

How Traffic Prioritization Works

Traffic prioritization uses the four traffic queues that are present in your device to ensure that high priority traffic is forwarded on a different queue from lower priority traffic. This is what provides Quality of Service (QoS) to your network.

The switch traffic prioritization depends on two industry-standard methods:

- **IEEE 802.1D**—a layer 2 marking scheme.
- **Differentiated Services (DiffServ)**—a layer 3 marking scheme.

IEEE 802.1D Traffic Marking

The IEEE Std 802.1D, 1998 Edition marking scheme, which is an enhancement to IEEE Std 802.1D, enables Quality of Service on the LAN. Traffic service levels are defined in the IEEE 802.1Q 4-byte tag, which is used to carry VLAN identification as well as IEEE 802.1p priority information. The 4-byte tag immediately follows the destination MAC address and Source MAC address.

The IEEE Std 802.1D, 1998 Edition priority marking scheme assigns an IEEE 802.1p priority level between 0 and 7 to each frame. This determines the level of service that type of traffic should receive. Refer to the table below for an example of how different traffic types can be mapped to the eight IEEE 802.1p priority levels.

IEEE 802.1p Priority Level	IEEE 802.1D Traffic Type
0	Best Effort (default)
1	Background
2	Standard (spare)
3	Excellent Effort (business critical)
4	Controlled Load (streaming multimedia)
5	Video (interactive media); less than 100 milliseconds of latency and jitter
6	Voice (interactive voice); less than 10 milliseconds of latency and jitter
7	Network Control Reserved traffic

Even though the IEEE 802.1D standard is the most widely used prioritization scheme in the LAN environment, it still has some restrictions:

- It requires an additional 4-byte tag in the frame, which is normally optional in Ethernet networks. Without this tag, the scheme cannot work.
- The tag is part of the IEEE 802.1Q header, so to implement QoS at layer 2, the entire network must implement IEEE 802.1Q VLAN tagging.

It is only supported on a LAN and not across routed WAN links, since the IEEE 802.1Q tags are removed when the packets pass through a router.

Differentiated Services (DiffServ) Traffic Marking

DiffServ is a Layer 3 marking scheme that uses the DiffServ Code Point (DSCP) field in the IP header to store the packet priority information. DSCP is an advanced intelligent method of traffic marking because you can choose how your network prioritizes different types of traffic. DSCP uses 64 values that map to user-defined service levels, allowing you to establish more control over network traffic.

Advantages of DiffServ over IEEE 802.1D are:

- Configure how you want your switch to treat selected applications and types of traffic by assigning various grades of network service to them.
- No extra tags are required in the packet.
- DSCP uses the IP header of a packet and therefore priority is preserved across the Internet.

- DSCP is backward compatible with IPV4 TOS, which allows operation with existing devices that use a layer 3 TOS enabled prioritization scheme.

Traffic Prioritization

The IE-SW-VL08M classifies traffic based on layer 2 of the OSI 7 layer model, and the switch prioritizes received traffic according to the priority information defined in the received packet. Incoming traffic is classified based upon the IEEE 802.1D frame and is assigned to the appropriate priority queue based on the IEEE 802.1p service level value defined in that packet. Service level markings (values) are defined in the IEEE 802.1Q 4-byte tag, and consequently traffic will only contain 802.1p priority markings if the network is configured with VLANs and VLAN tagging. The traffic flow through the switch is as follows:

1. A packet received by the switch may or may not have an 802.1p tag associated with it. If it does not, then it is given a default 802.1p tag (which is usually 0). Alternatively, the packet may be marked with a new 802.1p value, which will result in all knowledge of the old 802.1p tag being lost.
2. Because the 802.1p priority levels are fixed to the traffic queues, the packet will be placed in the appropriate priority queue, ready for transmission through the appropriate egress port. When the packet reaches the head of its queue and is about to be transmitted, the device determines whether or not the egress port is tagged for that VLAN. If it is, then the new 802.1p tag is used in the extended 802.1D header.

The switch will check a packet received at the ingress port for IEEE 802.1D traffic classification, and then prioritize it based upon the IEEE 802.1p value (service levels) in that tag. It is this 802.1p value that determines which traffic queue the packet is mapped to.

Traffic Queues

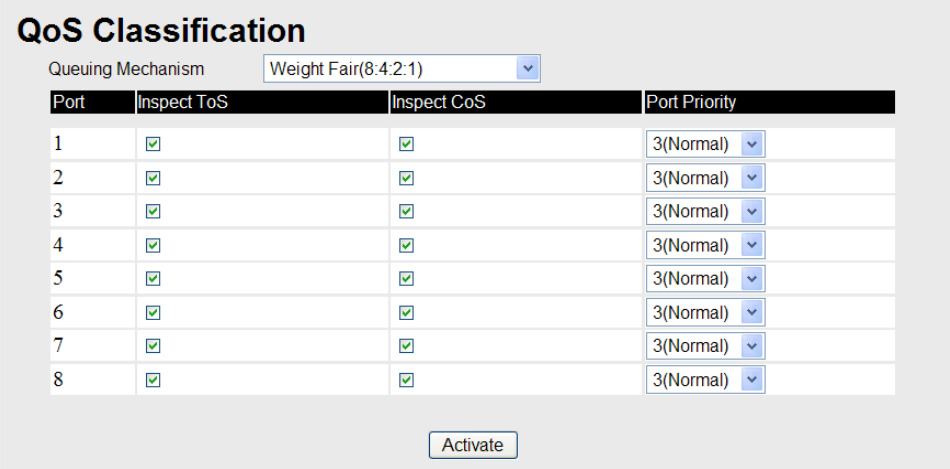
The IE-Sw-VL08M hardware has multiple traffic queues that allow packet prioritization to occur. Higher priority traffic can pass through the device without being delayed by lower priority traffic. As each packet arrives in the device, it passes through any ingress processing (which includes classification, marking/re-marking), and is then sorted into the appropriate queue. The switch then forwards packets from each queue.

The IE-SW-VL08M supports two different queuing mechanisms:

- **Weight Fair:** This method services all the traffic queues, giving priority to the higher priority queues. Under most circumstances, this method gives high priority precedence over low-priority, but in the event that high-priority traffic exceeds the link capacity, lower priority traffic is not blocked.
- **Strict:** This method services high traffic queues first; low priority queues are delayed until no more high priority data needs to be sent. This method always gives precedence to high priority over low-priority.

Configuring Traffic Prioritization

QoS Classification



The IE-SW-VL08M supports inspection of layer 3 TOS and/or layer 2 QoS tag information to determine how to classify traffic packets. (**NOTE:** The user interface for the IE-SW-VL08M shows 8 ports.)

Queuing Mechanism

Setting	Description	Factory Default
Weighted Fair	The Ethernet Switch has 4 priority queues. In the weight fair scheme, an 8, 4, 2, 1 weighting is applied to the four priorities. This approach prevents the lower priority frames from being starved of opportunity for transmission with only a slight delay to the higher priority frames.	Weight Fair
Strict	In the Strict-priority scheme, all top-priority frames egress a port until that priority's queue is empty, and then the next lower priority queue's frames egress. This approach can cause the lower priorities to be starved of opportunity for transmitting any frames but ensures all high priority frames to egress the switch as soon as possible.	

Inspect TOS

Setting	Description	Factory Default
Enable/Disable	Select this setting to enable the IE-SW-VL08M to inspect the Type of Service (TOS) bits in IPV4 frame to determine the priority of each frame.	Enable

Inspect COS

Setting	Description	Factory Default
Enable/Disable	Select this setting to enable the IE-SW-VL08M to inspect the 802.1p COS tag in the MAC frame to determine the priority of each frame.	Enable

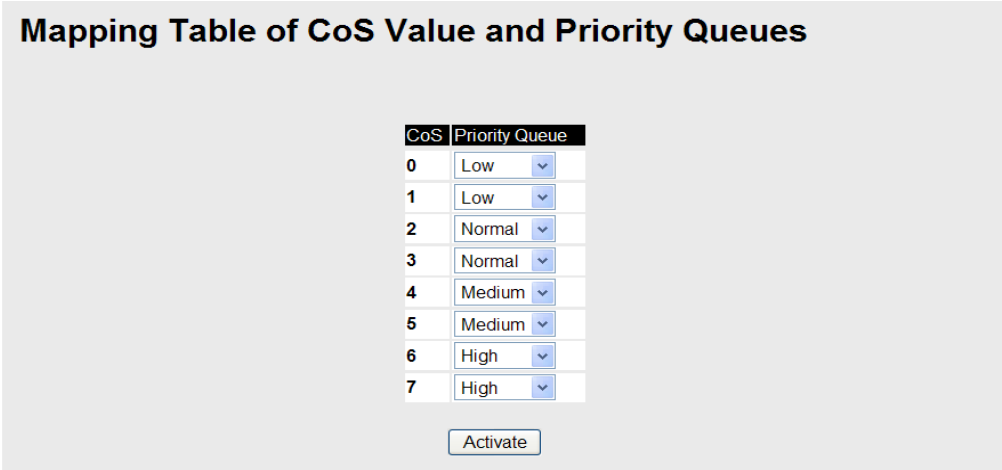
Default Port Priority

Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the Port Default Priority of the ingress frames to different priority queues. If the received packets are not equipped with any tag information (CoS, TOS) the default port priority will take effect.	Normal

NOTE The priority of an ingress frame is determined in order by:

1. Inspect TOS
2. Inspect CoS
3. Default Port Priority

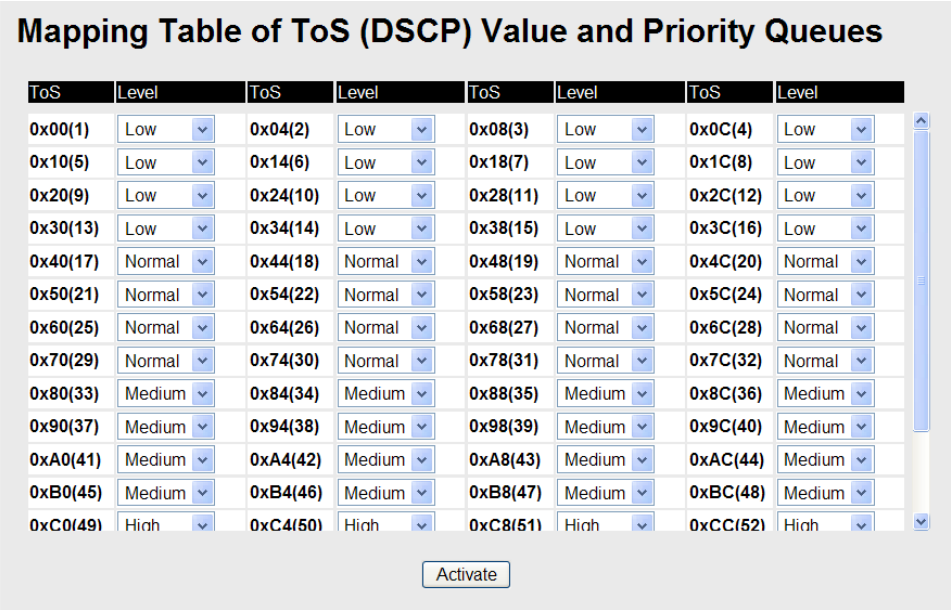
NOTE The designer can enable these classifications individually or in combination. For instance, if a 'hot' higher priority port is required for a network design, ***Inspect TOS*** and ***Inspect CoS*** can be disabled. This setting leaves only port default priority active, which results in all ingress frames being assigned the same priority on that port.



CoS Mapping

Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the mapping table of different CoS values to 4 different egress queues.	0: Low 1: Low 2: Normal 3: Normal 4: Medium 5: Medium 6: High 7: High

TOS/DiffServ Mapping


Mapping Table of ToS (DSCP) Value and Priority Queues
ToS Level ToS Level ToS Level ToS Level
0x00(1) Low 0x04(2) Low 0x08(3) Low 0x0C(4) Low
0x10(5) Low 0x14(6) Low 0x18(7) Low 0x1C(8) Low
0x20(9) Low 0x24(10) Low 0x28(11) Low 0x2C(12) Low
0x30(13) Low 0x34(14) Low 0x38(15) Low 0x3C(16) Low
0x40(17) Normal 0x44(18) Normal 0x48(19) Normal 0x4C(20) Normal
0x50(21) Normal 0x54(22) Normal 0x58(23) Normal 0x5C(24) Normal
0x60(25) Normal 0x64(26) Normal 0x68(27) Normal 0x6C(28) Normal
0x70(29) Normal 0x74(30) Normal 0x78(31) Normal 0x7C(32) Normal
0x80(33) Medium 0x84(34) Medium 0x88(35) Medium 0x8C(36) Medium
0x90(37) Medium 0x94(38) Medium 0x98(39) Medium 0x9C(40) Medium
0xA0(41) Medium 0xA4(42) Medium 0xA8(43) Medium 0xAC(44) Medium
0xB0(45) Medium 0xB4(46) Medium 0xB8(47) Medium 0xBC(48) Medium
0xC0(49) High 0xC4(50) High 0xC8(51) High 0xCC(52) High
Activate

Setting	Description	Factory Default
Low/Normal/ Medium/High	Set the mapping table of different TOS values to 4 different egress queues.	1 to 16: Low 17 to 32: Normal 33 to 48: Medium 49 to 64: High

Using Virtual LANs

Setting up Virtual LANs (VLANs) on your device increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

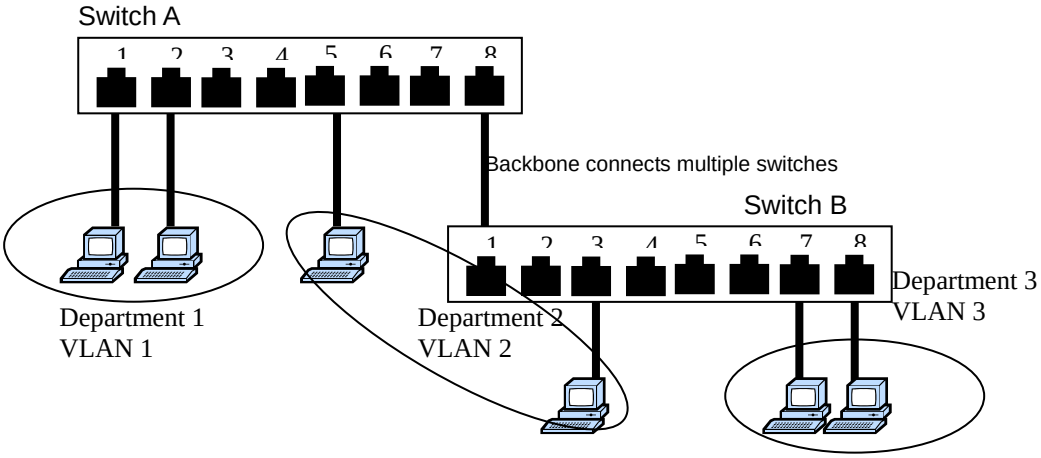
The Virtual LAN (VLAN) Concept

What is a VLAN?

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, you can segment your network without being restricted by physical connections—a limitation of traditional network design. As an example,

with VLANs you can segment your network according to:

- **Departmental groups**—You could have one VLAN for the Marketing department, another for the Finance department, and another for the Development department.
- **Hierarchical groups**—You could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—You could have one VLAN for e-mail users, and another for multimedia users.



Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides you with three other benefits:

- **VLANs ease the relocation of devices on networks:** With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each host must be updated manually. With a VLAN setup, if a host on VLAN *Marketing*, for example, is moved to a port in another part of the network, and retains its original subnet membership, you only need to specify that the new port is on VLAN *Marketing*. You do not need to do any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on VLAN *Marketing* needs to communicate with devices on VLAN *Finance*, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether or not they need it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that need to communicate with each other.

VLANs and Weidmueller Industrial Ethernet Switch's

Your IE-SW-VL08M provides support for VLANs using IEEE Std 802.1Q-1998. This standard allows traffic from multiple VLANs to be carried across one physical link. The IEEE Std 802.1Q-1998 standard allows each port on your device to be placed in:

- Any one VLAN defined on the IE-SW-VL08M.
- Several VLANs at the same time using 802.1Q tagging.

The standard requires that you define the *802.1Q VLAN ID* for each VLAN on your IE-SW-VL08M before the switch can use it to forward traffic:

Managing a VLAN

A new or initialized switch contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- *VLAN Name*—Management VLAN
- *802.1Q VLAN ID*—1 (if tagging is required)

All the ports are initially placed on this VLAN, and it is the only VLAN that allows you to access the management software of the IE-SW-VL08M over the network.

Communication between VLANs

If devices connected to a VLAN need to communicate to devices on a different VLAN, a router or Layer 3 switching device with connections to both VLANs needs to be installed. Communication between VLANs can only take place if they are all connected to a routing or Layer 3 switching device.

VLANs: Tagged and Untagged Membership

The IE-SW-VL08M supports 802.1Q VLAN tagging, a system that allows traffic for multiple VLANs to be carried on a single physical (backbone, trunk) link. When setting up VLANs you need to understand when to use untagged and tagged membership of VLANs. Simply put, if a port is on a single VLAN it can be an untagged member, but if the port needs to be a member of multiple VLANs, tagged membership must be defined.

A typical host (e.g., clients) will be untagged members of one VLAN, defined as "Access Port" in the switch, while inter-switch connections will be tagged members of all VLANs, defined as "Trunk Port" in the IE-SW-VL08M.

The IEEE Std 802.1Q-1998 defines how VLANs operate within an open packet-switched network. An 802.1Q compliant packet carries additional information that allows a switch to determine which VLAN the port belongs. If a frame is carrying the additional information, it is known as a *tagged* frame.

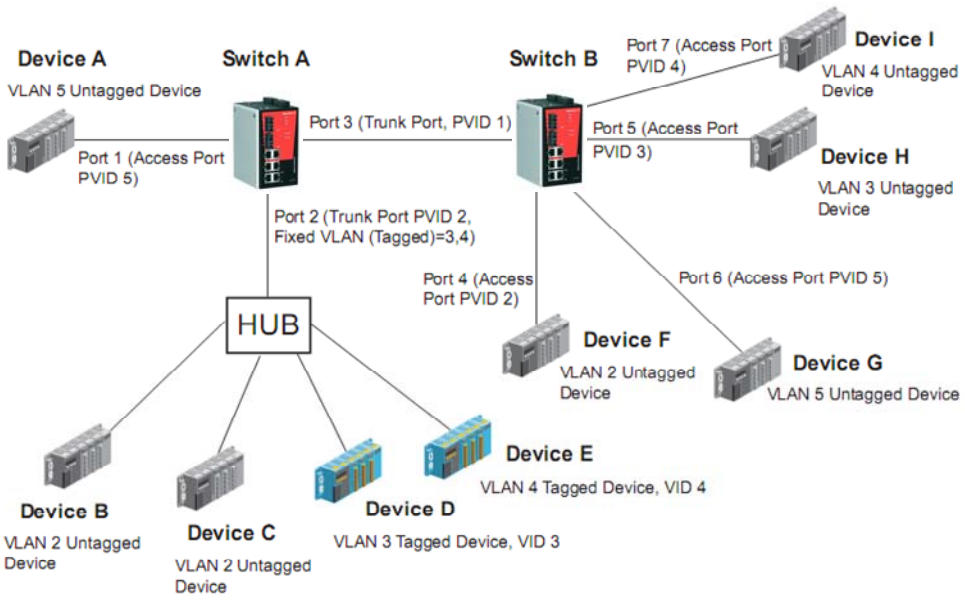
To carry multiple VLANs across a single physical (backbone, trunk) link, each packet must be tagged with a VLAN identifier so that the switches can identify which packets belong to which VLAN. To communicate between VLANs, a router must be used.

The IE-SW-VL08M supports two types of VLAN port settings:

- **Access Port:** The port connects to a single device that is not tagged. The user must define the default port PVID that determines to which VLAN the device belongs. Once the ingress packet of this Access Port egresses to another Trunk Port (the port needs all packets to carry tag information), the IE-SW-VL08M will insert this PVID into this packet to help the next 802.1Q VLAN switch recognize it.
- **Trunk Port:** The port connects to a LAN that consists of untagged devices/tagged devices and/or switches and hubs. In general, the traffic of the Trunk Port must have a Tag. Users can also assign PVID to a Trunk Port. The untagged packet on the Trunk Port will be assigned the port default PVID as its VID.

The following section illustrates how to use these ports to set up different applications.

Sample Applications of VLANs using the IE-SW-VL08M



In this application,

- Port 1 connects a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 2 connects a LAN with two untagged devices belonging to VLAN 2. One tagged device with VID 3 and one tagged device with VID 4. It should be configured as "Trunk Port" with PVID 2 for untagged device and Fixed VLAN (Tagged) with 3 and 4 for tagged device. Since each port can only have one unique PVID, all untagged devices on the same port can only belong to the same VLAN.
- Port 3 connects with another switch. It should be configured as "Trunk Port." GVRP protocol will be used through the Trunk Port.
- Port 4 connects a single untagged device and assigns it to VLAN 2; it should be configured as "Access Port" with PVID 2.
- Port 5 connects a single untagged device and assigns it to VLAN 3; it should be configured as "Access Port" with PVID 3.
- Port 6 connect a single untagged device and assigns it to VLAN 5; it should be configured as "Access Port" with PVID 5.
- Port 7 connects a single untagged device and assigns it to VLAN 4; it should be configured as "Access Port" with PVID 4.

After proper configuration:

- Packets from device A will travel through "Trunk Port 3" with tagged VID 5. Switch B will recognize its VLAN, pass it to port 6, and then remove tags received successfully by device G, and vice versa.
- Packets from device B and C will travel through "Trunk Port 3" with tagged VID 2. Switch B recognizes its VLAN, passes it to port 4, and then removes tags received successfully by device F, and vice versa.
- Packets from device D will travel through "Trunk Port 3" with tagged VID 3. Switch B will recognize its VLAN, pass to port 5, and then remove tags received successfully by device H.

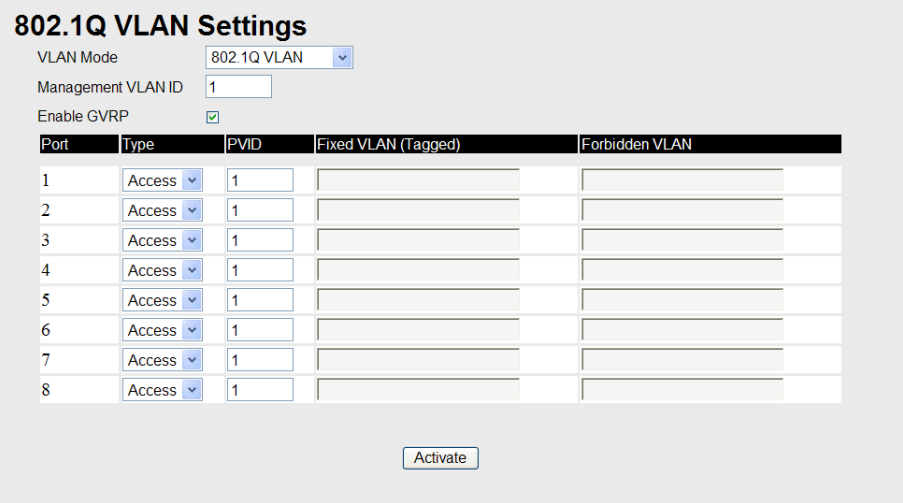
Packets from device H will travel through "Trunk Port 3" with PVID 3. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device D.

- Packets from device E will travel through "Trunk Port 3" with tagged VID 4. Switch B will recognize its VLAN, pass it to port 7, and then remove tags received successfully by device I. Packets from device I will travel through "Trunk Port 3" with tagged VID 4. Switch A will recognize its VLAN and pass it to port 2, but will not remove tags received successfully by device E.

Configuring Virtual LAN

VLAN Settings

To configure the IE-SW-VL08M's **802.1Q VLAN**, use the VLAN Setting page to configure the ports.



VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

Management VLAN ID

Setting	Description	Factory Default
VLAN ID ranges from 1 to 4094	Set the management VLAN of this Ethernet Switch	1

Enable GVRP

Setting	Description	Factory Default
Enable/Disable	Select the option to enable/disable the GVRP function.	Enable

Port Type

Setting	Description	Factory Default
Access	This port type is used to connect single devices without tags.	Access
Trunk	Select "Trunk" port type to connect another 802.1Q VLAN aware switch or another LAN that combines	

	tagged and/or untagged devices and/or other switches/hubs.	

ATTENTION

For communication redundancy in the VLAN environment, set "Redundant Port," "Coupling Port," and "Coupling Control Port" as "Trunk Port," since these ports act as the "backbone" to transmit all packets of different VLANs to different Ethernet Switches.

Port PVID

Setting	Description	Factory Default
VID range from 1 to 4094	Set the port default VLAN ID for untagged devices that connect to the port.	1

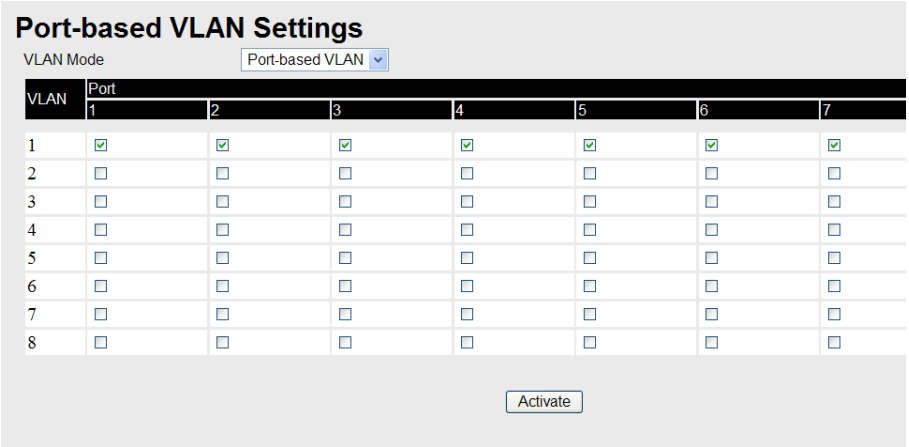
Fixed VLAN List (Tagged)

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the "Trunk" port type. Set the other VLAN ID for tagged devices that connect to the "Trunk" port. Use commas to separate different VIDs.	*None*

Forbidden VLAN List

Setting	Description	Factory Default
VID range from 1 to 4094	This field will be active only when selecting the "Trunk" port type. Set the VLAN IDs that will not be supported by this trunk port. Use commas to separate different VIDs.	*None*

To configure the **Port-based VLAN**, use the VLAN Setting page to configure the ports.



VLAN Mode

Setting	Description	Factory Default
802.1Q VLAN	Set VLAN mode to 802.1Q VLAN	802.1Q VLAN
Port-based VLAN	Set VLAN mode to Port-based VLAN	

Port

Setting	Description	Factory Default
Enable/Disable	Set port to specific VLAN Group.	Enable (all ports belong to VLAN1)

VLAN Table

VLAN Table
VLAN Mode
VLAN Mode 802.1Q VLAN
Management VLAN
Management VLAN 1
Current 802.1Q VLAN List
Index VID Joined Access Port Joined Trunk Port
1 1 1, 2, 3, 4, 5, 6, 7, 8,

In 802.1Q VLAN table, you can review the VLAN groups that were created, Joined Access Ports, and Trunk Ports, and in Port-based VLAN table, you can review the VLAN group and Joined port.

NOTE The physical network can have a maximum of 64 VLAN settings.

Using Multicast Filtering

Multicast filtering improves the performance of networks that carry multicast traffic. This section explains multicasts, multicast filtering, and how multicast filtering can be implemented on your IE-SW-VL08M.

The Concept of Multicast Filtering

What is an IP Multicast?

A *multicast* is a packet sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. If the network is set up correctly, a multicast can only be sent to an end-station or a subset of end-stations on a LAN or VLAN that belong to the multicast group. Multicast group members can be distributed across multiple subnets, so that multicast transmissions can occur within a campus LAN or over a WAN. In addition, networks that support IP multicast send only *one* copy of the desired information across the network until the delivery path that reaches group members diverges. To make more efficient use of network bandwidth, it is only at these points that multicast packets are duplicated and forwarded. A multicast packet has a multicast group address in the destination address field of the packet's IP header.

Benefits of Multicast

The benefits of using IP multicast are that it:

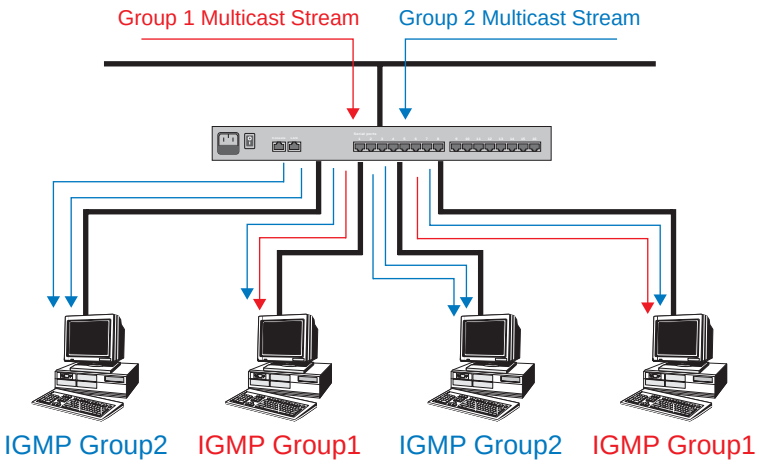
- Uses the most efficient, sensible method to deliver the same information to many receivers with only one transmission.
- Reduces the load on the source (for example, a server) since it will not need to produce several copies of the same data.
- Makes efficient use of network bandwidth and scales well as the number of multicast group members increases.
- Works with other IP protocols and services, such as Quality of Service (QoS).

Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all end-stations would cause a substantial reduction in network performance. Furthermore, several industrial automation protocols, such as Allen-Bradley, EtherNet/IP, Siemens Profibus, and Foundation Fieldbus HSE (High Speed Ethernet), use multicast. These industrial Ethernet protocols use publisher/subscriber communications models by multicasting packets that could flood a network with heavy traffic. IGMP Snooping is used to prune multicast traffic so that it travels only to those end destinations that require the traffic, reducing the amount of traffic on the Ethernet LAN.

Multicast Filtering

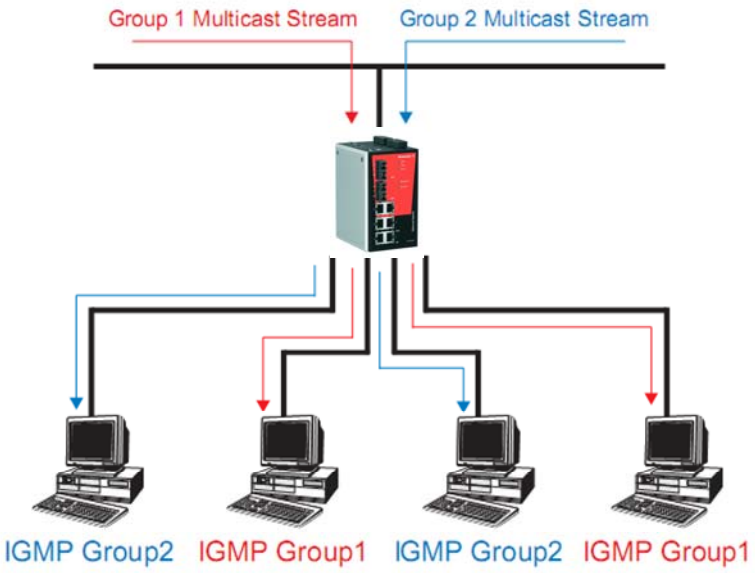
Multicast filtering ensures that only end-stations that have joined certain groups receive multicast traffic. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

Network without multicast filtering



All hosts receive the multicast traffic, even if they don't need it.

Network with multicast filtering



Hosts only receive dedicated traffic from other hosts belonging to the same group.

Multicast Filtering and IE-SW-VL08M Switch

The Ethernet Switch has three ways to achieve multicast filtering: IGMP (Internet Group Management Protocol) Snooping, GMRP (GARP Multicast Registration Protocol), and adding a static multicast MAC manually to filter multicast traffic automatically.

IGMP (Internet Group Management Protocol)

Snooping Mode

Snooping Mode allows your switch to forward multicast packets only to the appropriate ports. The switch "snoops" on exchanges between hosts and an IGMP device, such as a router, to find those ports that want to join a multicast group, and then configures its filters accordingly.

Query Mode

Query mode allows the Ethernet Switch to work as the Querier if it has the lowest IP address on the subnetwork to which it belongs. IGMP querying is enabled by default on the device to help prevent interoperability issues with some multicast routers that may not follow the lowest IP address election method. Enable query mode to run multicast sessions on a network that does not contain IGMP routers (or queriers).

NOTE The IE-SW-VL08M is compatible with any device that conforms to the IGMP v2 device protocol.

IGMP Multicast Filtering

IGMP is used by IP-supporting network devices to register hosts with multicast groups. It can be used on all LANs and VLANs that contain a multicast capable IP router, and on other network devices that support multicast filtering. IGMP works as follows:

1. The IP router (or querier) periodically sends *query* packets to all end-stations on the LANs or

VLANs that are connected to it. For networks with more than one IP router, the router with the lowest IP address is the querier. A switch with IP address lower than the IP address of any other IGMP queriers connected to the LAN or VLAN can become the IGMP querier.

2. When an IP host receives a query packet, it sends a *report* packet back that identifies the multicast group that the end-station would like to join.
3. When the report packet arrives at a port on a switch with *IGMP Snooping* enabled, the switch knows that the port should forward traffic for the multicast group, and then proceeds to forward the packet to the router.
4. When the router receives the report packet, it registers that the LAN or VLAN requires traffic for the multicast groups.
5. When the router forwards traffic for the multicast group to the LAN or VLAN, the switches only forward the traffic to ports that received a report packet.

GMRP (GARP Multicast Registration Protocol)

The IE-SW-VL08M supports IEEE 802.1D-1998 GMRP (GARP Multicast Registration Protocol), which differs from IGMP (Internet Group Management Protocol). GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or de-register Group membership information dynamically. GMRP functions similarly to GVRP, except that GMRP registers multicast addresses on ports. When a port receives a ***GMRP-join*** message, it will register the multicast address to its database if the multicast address is not registered, and all the multicast packets with that multicast address are able to be forwarded from this port. When a port receives a ***GMRP-leave*** message, it will de-register the multicast address from its database, and all the multicast packets with this multicast address are not able to be forwarded from this port.

Static Multicast MAC

Some devices may only support multicast packets, but not support either IGMP Snooping or GMRP. The IE-SW-VL08M supports adding multicast groups manually to enable multicast filtering.

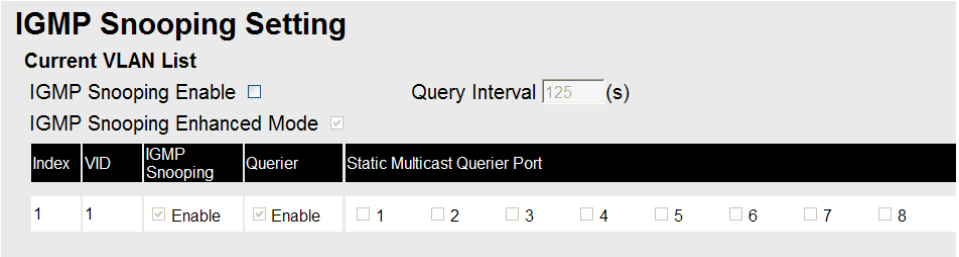
Enabling Multicast Filtering

Use the serial console or Web interface to enable or disable IGMP Snooping and IGMP querying. If IGMP Snooping is not enabled, then IP multicast traffic is always forwarded, flooding the network.

Configuring IGMP Snooping

IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN.

IGMP Snooping Settings



IGMP Snooping Enable

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the IGMP Snooping function **globally**.	Disabled

IGMP Snooping Enhanced Mode

Setting	Description	Factory Default
Enable	IGMP Multicast packets will forward to : • Learned Multicast Querier Ports • Member Ports	Enable
Disable	IGMP Multicast packets will forward to : • Learned multicast Querier Ports • Static Multicast Querier Ports • Querier Connected Ports • Member Ports	

Query Interval

Setting	Description	Factory Default
Numerical value input by user	Set the query interval of the Querier function globally. Valid settings are from 20 to 600 seconds.	125 seconds

IGMP Snooping

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the IGMP Snooping function **per VLAN**.	Enabled if IGMP Snooping Enabled Globally

NOTE **We suggest the following IGMP Snooping configurations:**

- **When the network is mixed with third party switches, such as Cisco:**
  → Select IGMP Snooping Enable: ☑
  → Clear IGMP Snooping Enhanced Mode: ☐
- **When the network consists entirely of Weidmueller switches:**
  → Select IGMP Snooping Enable-☑
  → Select IGMP Snooping Enhanced Mode- ☑

Querier

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the querier function.	Enabled if IGMP Snooping is Enabled Globally

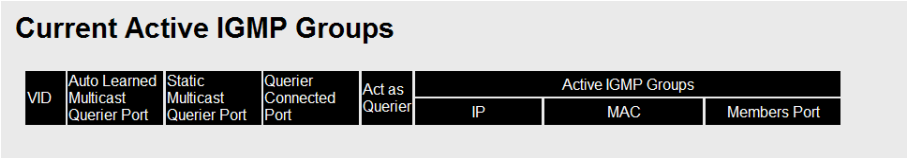
Static Multicast Router Port

Setting	Description	Factory Default
Select/Deselect	Select the option to select which ports will connect to the multicast routers. It's active only when IGMP Snooping is enabled.	Disabled

NOTE At least one switch must be designated the Querier or enable IGMP snooping and GMRP when enabling Turbo Ring and IGMP snooping simultaneously.

IGMP Table

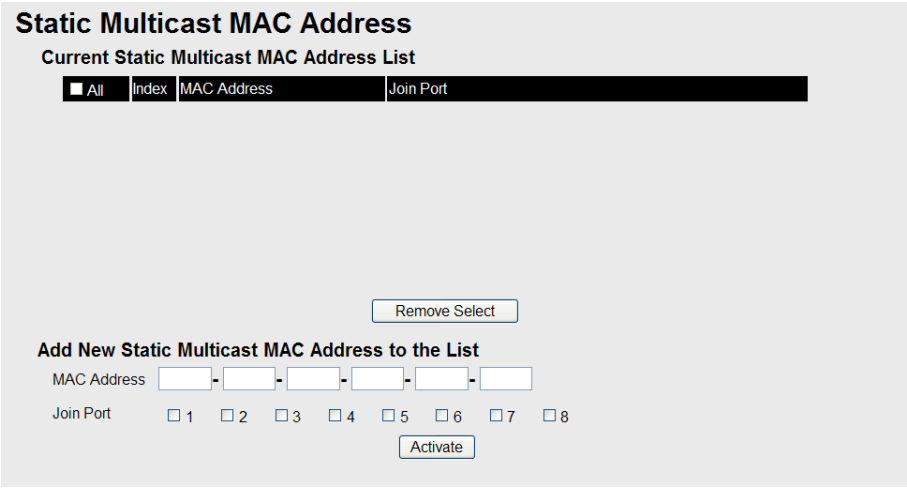
The IE-SW-VL08M displays the current active IGMP groups that were detected.



The information includes **VID**, **Auto-learned Multicast Router Port**, **Static Multicast Router Port**, **Querier Connected Port**, and the **IP** and **MAC** addresses of active IGMP groups.

Static Multicast MAC

The Ethernet switch also supports Multicast. If required, add multicast groups manually.



Add New Static Multicast Address to the List

Setting	Description	Factory Default
MAC Address	Input the multicast MAC address of this host.	*None*

MAC Address

Setting	Description	Factory Default
integer	Input the number of the VLAN to which the host with this MAC Address belongs.	*None*

Join Port

Setting	Description	Factory Default
Select/Deselect	Select the appropriate options to select the join ports for this multicast group.	*None*

Configuring GMRP

GMRP is a MAC-based multicast management protocol, whereas IGMP is IP-based. GMRP provides a mechanism that allows bridges and end stations to register or un-register Group membership information dynamically.

GMRP enable

Setting	Description	Factory Default
Enable/Disable	Select the option to enable the GMRP function for the port listed in the Port column	Disable

GMRP Table

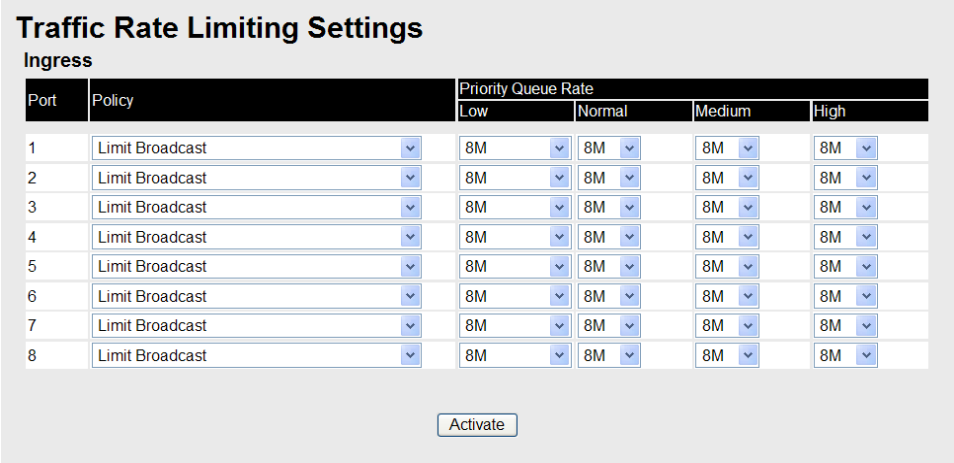
The IE-SW-VL08M displays the current active GMRP groups that were detected.

Setting	Description
Fixed Ports	This multicast address is defined by static multicast.
Learned Ports	This multicast address is learned by GMRP.

Using Rate Limiting

A single device should not be allowed to occupy unlimited bandwidth, especially when the device malfunctions. For example, broadcast storms could be caused by an incorrect topology or malfunctioning device. The IE-SW-VL08M devices not only prevents broadcast storms, but can also configure the ingress rate of unicast/multicast/broadcast packets, giving administrators full control of the limited bandwidth, and preventing unpredictable faults before they occur.

Configuring Rate Limiting



NOTE: The user interface for the IE-SW-VL08M **shows 8 ports.**

Policy

Setting	Description	Factory Default
Limit All	Selecting this option prohibits all traffic of broadcast, multicast, and unicast packets that exceed the rate set in the following "Rate" field.	Limit Broadcast
Limit Broadcast	Selecting this option prohibits all traffic of broadcast packets that exceed the rate set in the following "Rate" field.	
Limit Broadcast and Multicast	Selecting this option prohibits all traffic of broadcast and multicast packets that exceed the rate set in the following "Rate" field.	
Limit Broadcast, Multicast, and flooded unicast	Selecting this option prohibits all traffic of broadcast, multicast, and flooded unicast (new unicast addresses not learned by the IE-SW-VL08M packets that exceed the rate set in the following "Rate" field.	

Rate of Low Priority Queue

Setting	Description	Factory Default
Not limited, 128K, 256K, 512K, 1M, 2M, 4M, 8M	Set the threshold of traffic of limited packets in the IE-SW-VL08M's low priority queue.	8M

Rate of Normal Priority Queue

Setting	Description	Factory Default
The same or double rate of low priority queue	Set the threshold of traffic of limited packets in the IE-SW-VL08M's Normal priority queue.	8M

Rate of Medium Priority Queue

Setting	Description	Factory Default
The same or double rate of Normal priority queue	Set the threshold of traffic of limited packets in the IE-SW-VL08M's medium priority queue.	8M

Rate of High Priority Queue

Setting	Description	Factory Default
The same or double rate of medium priority queue	Set the threshold of traffic of limited packets in the IE-SW-VL08M's high priority queue.	8M

NOTE By default, the switch is configured to limit broadcast packets not to exceed 8M to protect against broadcast storms caused by careless usage. This value can be adjusted by the user.

Using Auto Warning

Since industrial Ethernet devices are often located at remote areas of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial Ethernet switch that connects to these devices must provide system maintainers with real-time warning messages. Even when control engineers are out of the control room for an extended period of time, they can still be informed of the status of devices almost instantaneously when exceptions occur. The IE-SW-VL08M supports different approaches such as email and relay output to warn engineers automatically.

Configuring Email Warning

The Auto Email Warning function uses e-mail to alert the user when certain user-configured events take place.

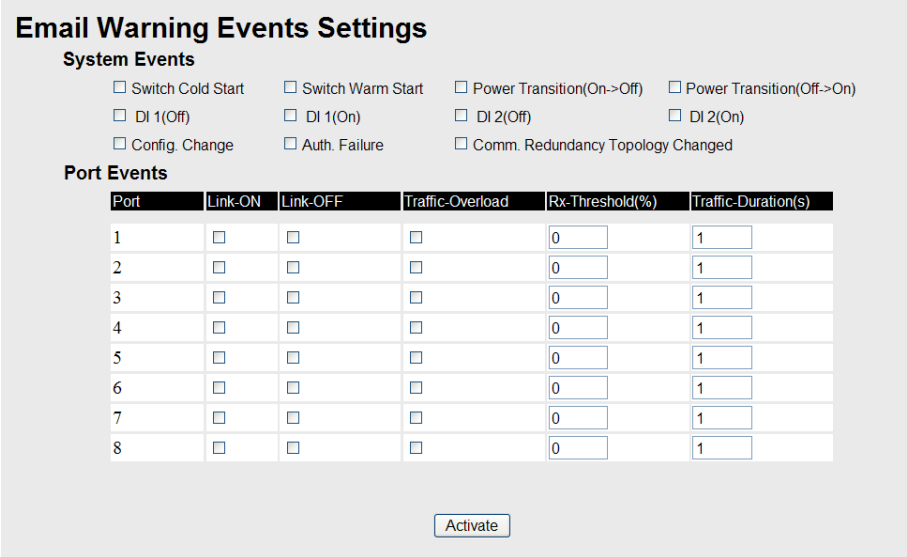
Three basic steps are required to set up the Auto Warning function:

1. **Configuring Email Event Types**
   Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Email Warning Events setting* subsection).

2. **Configuring Email Settings**
   To configure the IE-SW-VL08M's email setup from the Console interface or browser interface, enter your Mail Server IP/Name (IP address or name), Account Name, Account Password, Retype New Password, and the email address(es) to which warning messages will be sent.

3. **Activate your settings and test email if necessary**
   After configuring and activating your IE-SW-VL08M's Event Types and Email Setup, you can use the **Test Email** function to see if your e-mail addresses and mail server address have been properly configured.

Email Warning Events Settings



NOTE: The user interface for the IE-SW-VL08M **shows 8 ports.**

Event Types

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

System Event	Warning e-mail is sent when…
Switch Cold Start	Power is cut off and then reconnected.
Switch Warm Start	The device is rebooted, such as when network parameters are changed (IP address, netmask, etc.).
Power Transition (On→Off)	The device is powered down.
Power Transition (Off→On)	The device is powered up.
Configuration Change Activated	Any configuration item is changed.
Comm. Redundancy Topology Changed	If any Spanning Tree Protocol switches have changed their position (applies only to the root of the tree). If the Master of Turbo Ring has changed or backup path is activated.
Authentication Failure	An incorrect password is entered.

Port Event	Warning e-mail is sent when…
Link-on	The port is connected to another device.
Link-off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this setting is Enabled).

Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload setting is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every *Traffic-Duration* seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE The **Traffic-Overload**, **Traffic-Threshold (%)**, and **Traffic-Duration (sec.)** Port Event settings are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

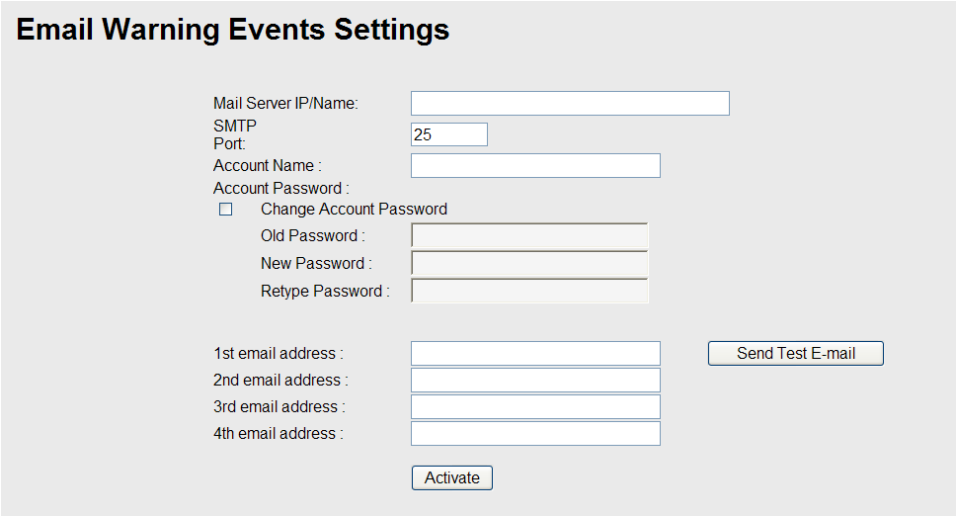
NOTE Warning e-mail messages will have the **sender** field in the form:

Weidmueller_IE-SW_Switch_0001@Switch_Location

where **Weidmueller_IE-SW_Switch** is the default Switch Name, **0001** is switches's serial number, and **Switch_Location** is the default Server Location.

Refer to the Basic **Settings** section to see how to modify Switch Name and Switch Location.

Email Settings



Mail Server IP/Name

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

Account Name

Setting	Description	Factory Default
Max. 45 Charters	Your email account.	None

Password Setting

Setting	Description	Factory Default
Disable/Enable to change Password	To reset the Password from the Web Browser interface, click the Change password check-box, type the Old Password, type the New Password, retype the New password, and then click Activate. The password can be a maximum of 45 characters.	Disable
Old Password	Type the current password when changing the password	None
New Password	Type new password when enabled to change password. The password can be a maximum of 45 characters.	None
Retype Password	If you type a new password in the Password field, you will be required to retype the password in the Retype new password field before updating the new password.	None

Email Address

Setting	Description	Factory Default
Max. 30 Characters	You can set up to 4 email addresses to receive warning emails from the IE-SW-VL08M.	None

Send Test Email

After finishing with the email settings, you should first press the ***Activate*** button to activate those settings, and then press the ***Send Test Email*** button to verify that the settings are correct.

NOTE Auto warning e-mail messages will be sent through an authentication protected SMTP server that supports the CRAM-MD5, LOGIN, and PAIN methods of SASL (Simple Authentication and Security Layer) authentication mechanism.

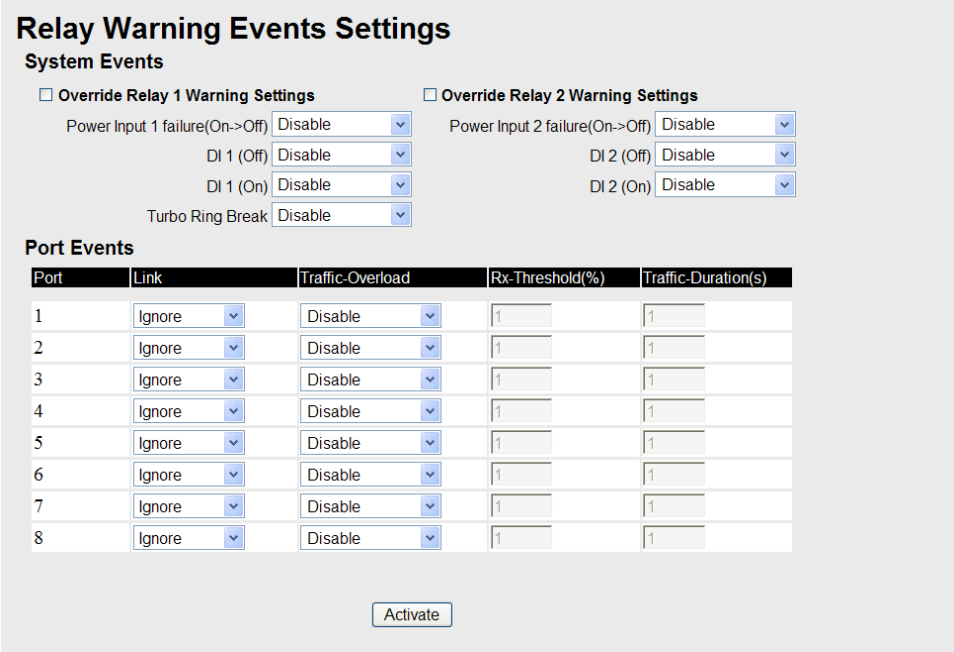
We strongly recommend not entering your Account Name and Account Password if auto warning e-mail messages can be delivered without authentication mechanism.

Configuring Relay Warning

The Auto Relay Warning function uses relay output to alert the user when certain user-configured events take place. There are two basic steps required to set up the Relay Warning function:

1. **Configuring Relay Event Types**
   Select the desired **Event types** from the Console or Web Browser Event type page (a description of each event type is given later in the *Relay Warning Events setting* subsection).
2. **Activate your settings**
   After configuring, you will need to activate your Weidmueller switch's Relay Event Types.

Relay Warning Events Settings


Relay Warning Events Settings
System Events
Override Relay 1 Warning Settings
Power Input 1 failure(On->Off) Disable
DI 1 (Off) Disable
DI 1 (On) Disable
Turbo Ring Break Disable
Override Relay 2 Warning Settings
Power Input 2 failure(On->Off) Disable
DI 2 (Off) Disable
DI 2 (On) Disable
Port Events
Port Link Traffic-Overload Rx-Threshold(%) Traffic-Duration(s)
1 Ignore Disable 1 1
2 Ignore Disable 1 1
3 Ignore Disable 1 1
4 Ignore Disable 1 1
5 Ignore Disable 1 1
6 Ignore Disable 1 1
7 Ignore Disable 1 1
8 Ignore Disable 1 1
Activate

NOTE: The user interface for the IE-SW-VL08M shows 8 ports.

Event Types

Event Types can be divided into two basic groups: **System Events** and **Port Events**. System Events are related to the overall function of the switch, whereas Port Events are related to the activity of a specific port.

The switch supports one relay output. You can configure which relay output is related to which events. This helps administrators identify the importance of the different events.

System Event	Warning Relay output is triggered when…
Power Transition (On→Off)	The device is powered up.
Power Transition (Off→On)	The device is powered down.
Turbo Ring Break (Ring Master Only)	When the IE-SW-VL08M is the Master of this Turbo Ring, and the Turbo Ring is disconnected.

NOTE If the Turbo Ring Switch function is enabled, and the Turbo Ring DIP Switch is set to "ON", the Turbo Ring Break Event cannot be changed. If not, the Turbo Ring Break Event can be set by using a web browser.

NOTE The Turbo Ring Break Warning will be automatically enabled when the following configuration is set:

1. Turbo Ring DIP Switch functions are enabled.
2. The Hardware Turbo Ring DIP Switch is set to "ON".

3. The Master DIP Switch is set to "ON".

Please refer to "Configuring Basic Settings—Turbo Ring DIP Switch" for more details.

Port Event	Warning e-mail is sent when…
Link-on	The port is connected to another device.
Link-off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Traffic-Overload	The port's traffic surpasses the Traffic-Threshold for that port (provided this setting is Enabled).
Traffic-Threshold (%)	Enter a nonzero number if the port's Traffic-Overload setting is Enabled.
Traffic-Duration (sec.)	A Traffic-Overload warning is sent every *Traffic-Duration* seconds if the average Traffic-Threshold is surpassed during that time period.

NOTE The **Traffic-Overload**, **Traffic-Threshold (%)**, and **Traffic-Duration (sec)** Port Event items are related. If you Enable the Traffic-Overload event, then be sure to enter a nonzero Traffic-Threshold percentage, as well as a Traffic-Duration between 1 and 300 seconds.

Override Relay Warning Settings

Click the checkbox to override the relay warning setting temporarily. Releasing the relay output will allow administrators to fix any problems with the warning condition.

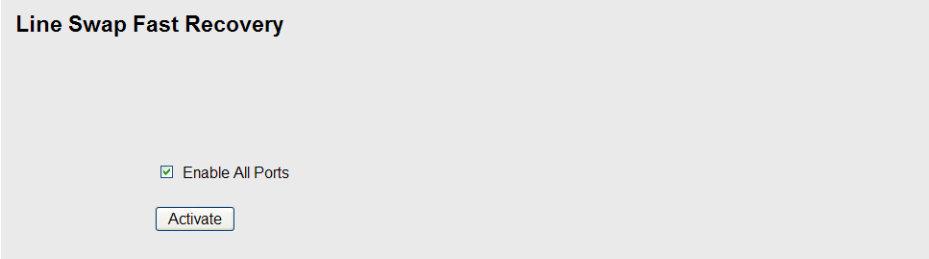
Relay Warning List

Use this table to see if any relay warnings have been issued.

Using Line-Swap-Fast-Recovery

The Line-Swap Fast Recovery function, which is enabled by default, allows the IE-SW-VL08M to return to normal operation very quickly after devices are unplugged and then re-plugged into different ports. The recovery time is in the order of a few milliseconds. Compare this with standard commercial switches for which the recovery time could be in the order of several minutes. To disable the Line-Swap Fast Recovery function, or to re-enable the function after it has already been disabled, access either the Console utility's **Line-Swap recovery** page, or the Web Browser interface's **Line-Swap fast recovery** page, as shown next.

Configuring Line-Swap Fast Recovery



Enable Line-Swap-Fast-Recovery

Setting	Description	Factory Default
Enable/Disable	Select this setting to enable the Line-Swap-Fast-Recovery function	Enable

Using Set Device IP

To reduce the effort required to set up IP addresses, the IE-SW-VL08M devices comes equipped with DHCP/BootP server and RARP protocol to set up IP addresses of Ethernet-enabled devices automatically.

When enabled, the **Set device IP** function allows the IE-SW-VL08M to assign specific IP addresses automatically to connected devices that are equipped with *DHCP Client* or *RARP* protocol. In effect, the IE-SW-VL08M acts as a DHCP server by assigning a connected device with a specific IP address stored in the switch's internal memory. Each time the connected device is switched on or rebooted, the IE-SW-VL08M sends the device the desired IP address.

Take the following steps to use the **Set device IP** function:

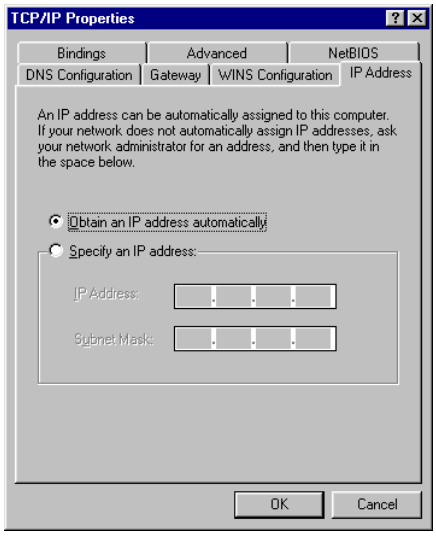
STEP 1—*set up the connected devices*

Set up the Ethernet-enabled devices connected to the IE-SW-VL08M for which you would like IP addresses to be assigned automatically. The devices must be configured to *obtain* their IP address automatically.

The devices' configuration utility should include a setup page that allows you to choose an option similar to **Obtain an IP address automatically**.

For example, Windows' **TCP/IP Properties** window is shown at the right. Although your device's configuration utility may look quite a bit different, this figure should give you some idea of what to look for.

You also need to decide which of the IE-SW-VL08M's ports your Ethernet-enabled devices will be connected to. You will need to set up each of these ports separately, as described in the next step.


TCP/IP Properties
Bindings
Advanced
NetBIOS
DNS Configuration
Gateway
WINS Configuration
IP Address
An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.
Obtain an IP address automatically
Specify an IP address:
IP Address:
Subnet Mask:
OK
Cancel

STEP 2

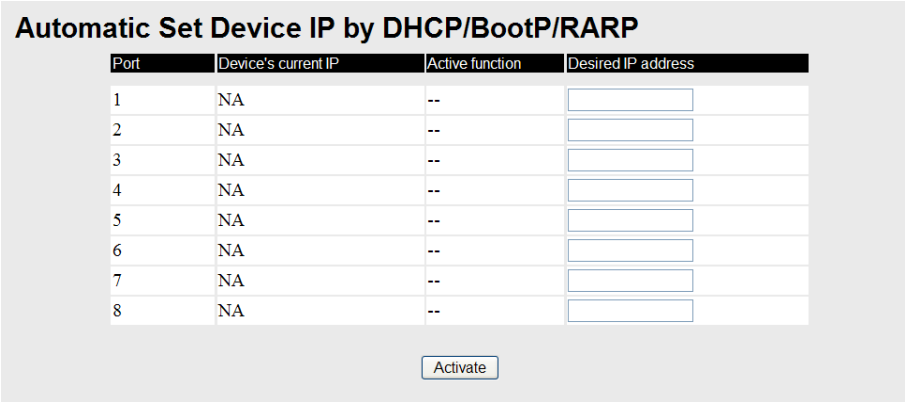
Configure the IE-SW-VL08M's **Set device IP** function, either from the Console utility or from the Web Browser interface. In either case, you simply need to enter the **Desired IP** for each port that needs to be configured.

STEP 3

Be sure to activate your settings before exiting.

- When using the Web Browser interface, activate by clicking the ***Activate*** button.
- When using the Console utility, activate by first highlighting the **Activate** menu option, and then press **Enter**. You should receive the **Set device IP settings are now active! (Press any key to continue)** message.

Configuring Set Device IP



NOTE: The user interface for IE-SW-VL08M **shows 8 ports.**

Desired IP Address

Setting	Description	Factory Default
IP Address	Set the desired IP of connected devices.	None

The DHCP Relay Agent makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

DHCP Relay Agent (Option 82)

Option 82 is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options: Circuit ID and Remote ID, which define the relationship between end device IP and the DHCP Option 82 server. The "Circuit ID" is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID. The format of the "Circuit ID" is as described below:

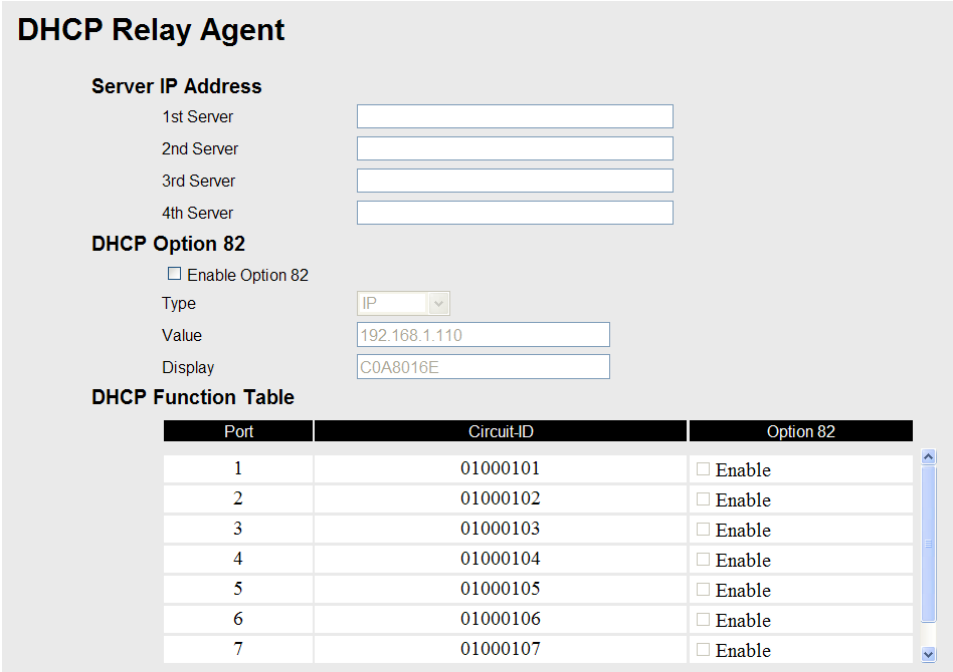
FF–VV–VV–PP

Where the first byte "FF" is fixed to "01", the second and the third byte "VV-VV" is formed by the port VLAN ID in hex, and the last byte "PP" is formed by the port number in hex. For example,

01–00–0F–03 is the "Circuit ID" of port number 3 with port VLAN ID 15.

The "Remote ID" is to identify the relay agent itself and it can be one of the following:

1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.
4. A user-defined string.



Server IP Address

1st Server

Setting	Description	Factory Default
IP address for the 1st DHCP server	This assigns the IP address of the 1st DHCP server that the switch tries to access.	None

2nd Server

Setting	Description	Factory Default
IP address for the 2nd DHCP server	This assigns the IP address of the 2nd DHCP server that the switch tries to access.	None

3rd Server

Setting	Description	Factory Default
IP address for the 3rd DHCP server	This assigns the IP address of the 3rd DHCP server that the switch tries to access.	None

4th Server

Setting	Description	Factory Default
IP address for the 4th DHCP server	This assigns the IP address of the 4th DHCP server that the switch tries to access.	None

DHCP Option 82

Enable Option82

Setting	Description	Factory Default
Enable or Disable	Enable or disable DHCP Option 82 function.	Disable

Type

Setting	Description	Factory Default
IP	Use switch IP address as the remote ID sub-option.	IP
MAC	Use switch MAC address as the remote ID sub-option.	IP
Client-ID	Use the combination of switch MAC address and IP address as the remote ID sub-option.	IP
Other	Use the user-defined value as the remote ID sub-option.	IP

Value

Setting	Description	Factory Default
	Displays the value which you've set.	
Max. 12 characters	If you set the type as Other, you will have to fill it.	switch IP address

Display

Setting	Description	Factory Default
	The actual hexdecimal value set at the DHCP server for the Remote-ID. This value is automatically generated according to the Value field. Users can not modify it.	COA87FFD

DHCP Function Table

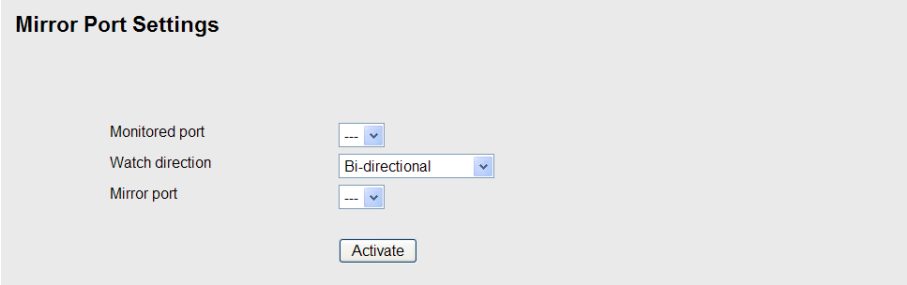
Enable

Setting	Description	Factory Default
Enable or Disable	Enable or disable DHCP Option 82 function for this port.	Disable

Using Diagnosis

The IE-SW-VL08M provides two important tools for administrators to diagnose network systems.

Mirror Port



The **Mirror port** function can be used to monitor data being transmitted through a specific port. This is done by setting up another port (the *mirror port*) to receive the same data being transmitted

from, or both to and from, the port under observation. This allows the network administrator to "sniff" the observed port and thus keep tabs on network activity.

Do the following to set up the **Mirror Port** function:

STEP 1

Configure the switch's **Mirror Port** function from either the Console utility or Web Browser interface. You will need to configure three settings:

Monitored Port Select the port number of the port whose network activity will be monitored.

Mirror Port Select the port number of the port that will be used to monitor the activity of the monitored port.

Watch Direction Select one of the following three watch direction options:

- **Input data stream**
  Select this option to monitor only those data packets coming *in through* the switch's port.
- **Output data stream**
  Select this option to monitor only those data packets being sent *out through* the switch's port.
- **Bi-directional**
  Select this option to monitor data packets both coming *into*, and being sent *out through*, the switch's port.

STEP 2

Be sure to activate your settings before exiting.

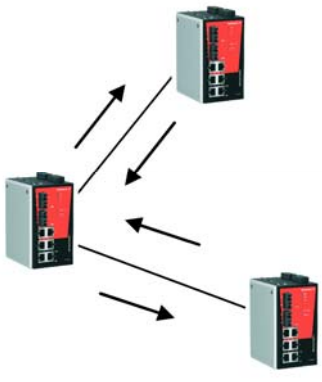
- When using the Web Browser interface, activate by clicking the ***Activate*** button.
- When using the Console utility, activate by first highlighting the Activate menu option, and then press **Enter**. You should receive the **Mirror port settings are now active! (Press any key to continue)** message.

Ping

The **Ping** function uses the *ping* command to give users a simple but powerful tool for troubleshooting network problems. The function's most unique feature is that even though the ping command is entered from the user's PC keyboard, the actual ping command originates from the device itself. In this way, the user can essentially control the device and send ping commands out through its ports.

To use the Ping function, type in the desired IP address, and then press **Enter** from the Console utility, or click **Ping** when using the Web Browser interface.

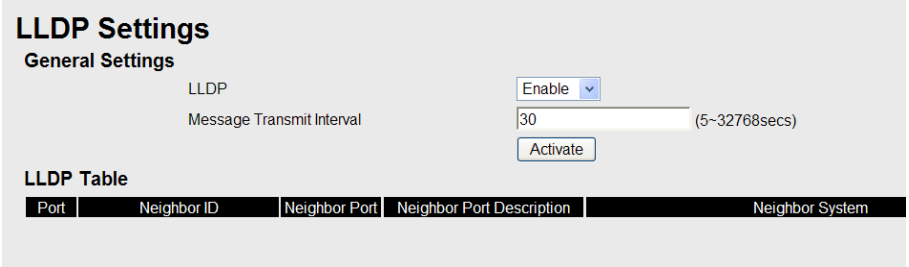
LLDP



Defined by IEEE 802.11AB, LLDP is an OSI Layer 2 Protocol that standardizes the methodology of self-identity advertisement. It allows each networking device, e.g. a Weidmueller's managed switch, to periodically inform its neighbors about its self-information and configurations. As a result, all of the devices will have knowledge about each other;

and through SNMP, this knowledge can be transferred to a Network Management Software for auto-topology and network visualization.

LLDP Web Interface



From the switch's web interface, users have the option of either enabling or disabling the LLDP, as well as setting the LLDP transmit interval (as shown in the figure below). In addition, users are able to view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows a Network Management Software to automatically display the network's topology as well as system setup details such as VLAN, and Trunking for the entire network.

LLDP Settings

Enable LLDP

Setting	Description	Factory Default
Enable or Disable	Enable or disable LLDP function.	Enable

Value

Setting	Description	Factory Default
Numbers from 5 to 32768 secs	To set the transmit interval of LLDP messages. Unit is in seconds.	30 (seconds)

LLDP Table

Port: The port number that connects to the neighbor device.

Neighbor ID: A unique entity which identifies a neighbor device; this is typically the MAC address.

Neighbor Port: The port number of the neighbor device.

Neighbor Port Description: A textual description of the neighbor device's interface.

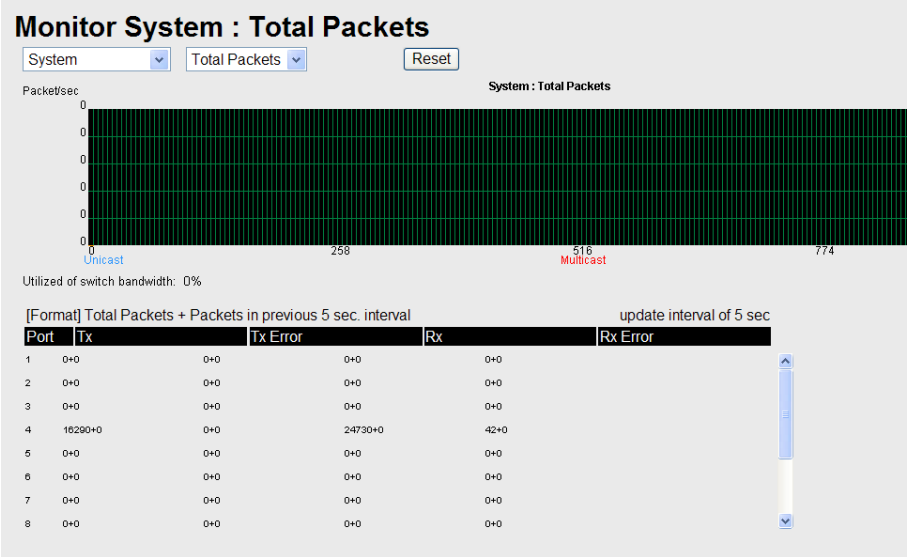
Neighbor System: Hostname of the neighbor device.

Using the Monitor

You can monitor statistics in real time from the IE-SW-VL08M's web console and serial console.

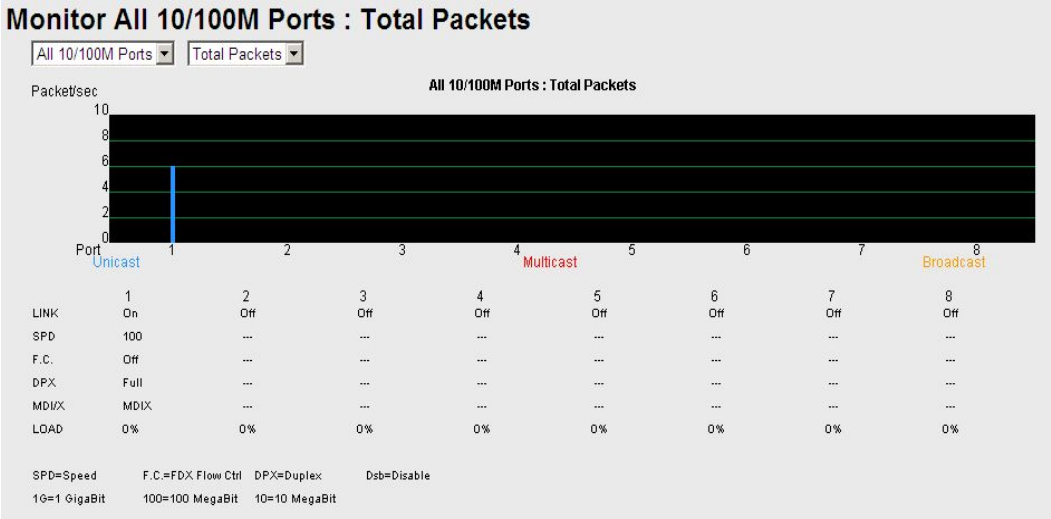
Monitor by Switch

Access the Monitor by selecting ***System*** from the left selection bar. Monitor by System allows the user to view a graph that shows the combined data transmission activity of all of the IE-SW-VL08M's ports. Click on one of the four options—Total Packets, TX Packets, RX Packets, or Error Packets—to view transmission activity of specific types of packets. Recall that TX Packets are packets sent out from the switch, RX Packets are packets received from connected devices, and Error Packets are packets that did not pass TCP/IP's error checking algorithm. The Total Packets option displays a graph that combines TX, RX, and Error Packet activity. The four graphs (Total Packets, TX Packets, RX Packets, and Error Packets) have the same form, so we show only the Total Packets graph here. The graph displays data transmission activity by showing **Packets/s** (i.e., packets per second, or pps) versus **sec.** (seconds). In fact, three curves are displayed on the same graph: **Uni-cast** packets (in red color), **Multi-cast** packets (in green color), and **Broad-cast** packets (in blue color). The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



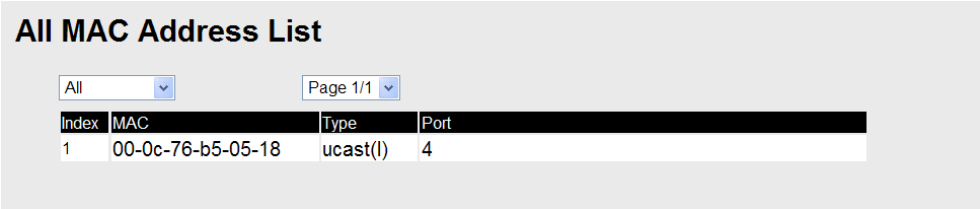
Monitor by Port

Access the Monitor by Port function by selecting **ALL 10/100M Ports** or **Port*i***, in which ***i***= 1, 2, … 8, etc., from the left pull-down list. The **Port*i*** options are identical to the Monitor by System function discussed previously, in that users can view graphs that show Total Packets, TX Packets, RX Packets, or Error Packets activity, but in this case, only for an individual port. The **All 10/100M Ports** option is essentially a graphical display of the individual port activity that can be viewed with the Console Monitor function discussed above. The All 10/100M Ports option shows three vertical bars for each port. The height of the bar represents **Packets/s** for the type of packet, at the instant the bar is being viewed. That is, as time progresses, the height of the bar moves up or down so that the user can view the change in the rate of packet transmission. The red colored bar shows **Uni-cast** packets, the green colored bar shows **Multi-cast** packets, and the blue colored bar shows **Broad-cast** packets. The graph is updated every few seconds, allowing the user to analyze data transmission activity in real-time.



Using the MAC Address Table

This section explains the information provided by the IE-SW-VL08M's MAC address table.



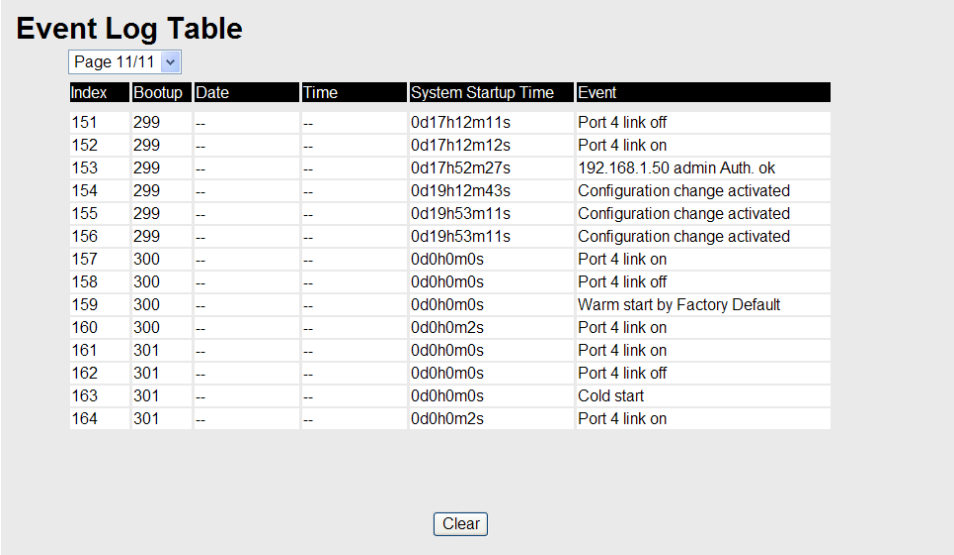
The MAC Address table can be configured to display the following IE-SW-VL08M MAC address groups.

ALL	Select this item to show all switch MAC addresses
ALL Learned	Select this item to show all switch Learned MAC addresses
ALL Static Multicast	Select this item to show all switch Static Multicast MAC addresses
Port x	Select this item to show all MAC addresses of dedicated ports

The table will display the following information:

MAC	This field shows the MAC address
Type	This field shows the type of this MAC address
Port	This field shows the port that this MAC address belongs to

Using Event Log


Event Log Table
Page 11/11
Index Bootup Date Time System Startup Time Event
151 299 -- -- 0d17h12m11s Port 4 link off
152 299 -- -- 0d17h12m12s Port 4 link on
153 299 -- -- 0d17h52m27s 192.168.1.50 admin Auth. ok
154 299 -- -- 0d19h12m43s Configuration change activated
155 299 -- -- 0d19h53m11s Configuration change activated
156 299 -- -- 0d19h53m11s Configuration change activated
157 300 -- -- 0d0h0m0s Port 4 link on
158 300 -- -- 0d0h0m0s Port 4 link off
159 300 -- -- 0d0h0m0s Warm start by Factory Default
160 300 -- -- 0d0h0m2s Port 4 link on
161 301 -- -- 0d0h0m0s Port 4 link on
162 301 -- -- 0d0h0m0s Port 4 link off
163 301 -- -- 0d0h0m0s Cold start
164 301 -- -- 0d0h0m2s Port 4 link on
Clear

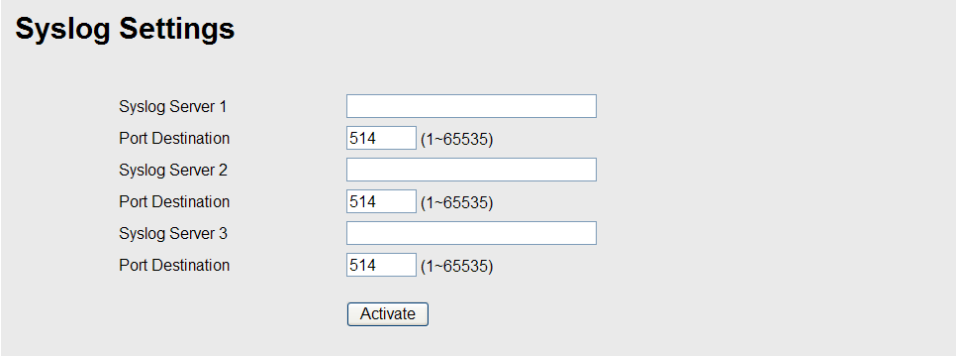
Bootup	This field shows how many times the IE-SW-VL08M has been rebooted or cold started.
Date	The date is updated based on how the current date is set in the "Basic Setting" page.
Time	The time is updated based on how the current time is set in the "Basic Setting" page.
System Startup Time	The system startup time related to this event.
Events	Events that have occurred.

Events are logged in the IE-SW-VL08M Event Log when the following events occur:

1. Cold start
2. Warm start
3. Configuration Change Activated
4. Power Transition from OFF to ON or from ON to OFF
5. Authentication Fail
6. Topology Changed
7. Master Setting is Mismatched
8. Port Traffic Overload
9. Port Link from OFF to ON or from ON to OFF

Using Syslog

This function provides the event logs for the syslog server. The function supports 3 configurable syslog servers and syslog server UDP port numbers. When an event occurs, the event will be sent as a syslog UDP packet to the specified syslog servers.



Syslog Server 1

Setting	Description	Factory Default
IP Address	Enter the IP address of 1st Syslog Server used by your network.	*None*
Port Destination (1 to 65535)	Enter the UDP port of 1st Syslog Server.	514

Syslog Server 2

Setting	Description	Factory Default
IP Address	Enter the IP address of 2nd Syslog Server used by your network.	*None*
Port Destination (1 to 65535)	Enter the UDP port of 2nd Syslog Server.	514

Syslog Server 3

Setting	Description	Factory Default
IP Address	Enter the IP address of 3rd Syslog Server used by your network.	*None*
Port Destination (1 to 65535)	Enter the UDP port of 3rd Syslog Server.	514

NOTE The following events will be recorded into the IE-SW-VL08M's Event Log table, and will then be sent to the specified Syslog Server:

1. Cold start
2. Warm start
3. Configuration change activated
4. Power 1/2 transition (Off → On), Power 1/2 transition (On → Off)
5. Authentication fail
6. Topology changed
7. Master setting is mismatched
8. DI 1/2 transition (Off → On), DI 1/2 transition (On → Off)
9. Port traffic overload
10. dot1x Auth Fail
11. Port link off / on

4

Weidmueller Switch Configuration Utility

The Weidmüller Switch configuration utility (WM_Switch_Utility.exe) is a comprehensive Windows-based GUI that can be used to configure and maintain multiple Weidmüller managed switches.

A suite of useful functions is available to help you

- → to locate Ethernet Switches which are attached to the same LAN as the PC host (regardless of whether or not you know the IP addresses of the switches),
- → to connect to an Ethernet Switch whose IP address is known,
- → to modify the network configurations of one or multiple Ethernet Switches
- → and to update the firmware of one or more Ethernet Switches.

The Weidmüller Switch Configuration Utility is designed to provide you with instantaneous control of your Ethernet Switches regardless of location. You may download the Weidmüller Switch Configuration Utility software from Weidmüller's website free of charge.

This chapter includes the following sections:

- ☐ Starting Weidmüller Switch Configuration Utility
- ☐ Broadcast Search
- ☐ Search by IP address
- ☐ Upgrade Firmware
- ☐ Modify IP Address
- ☐ Export Configuration
- ☐ Import Configuration
- ☐ Unlock the Ethernet Switch

Starting Weidmüller Switch Configuration Utility

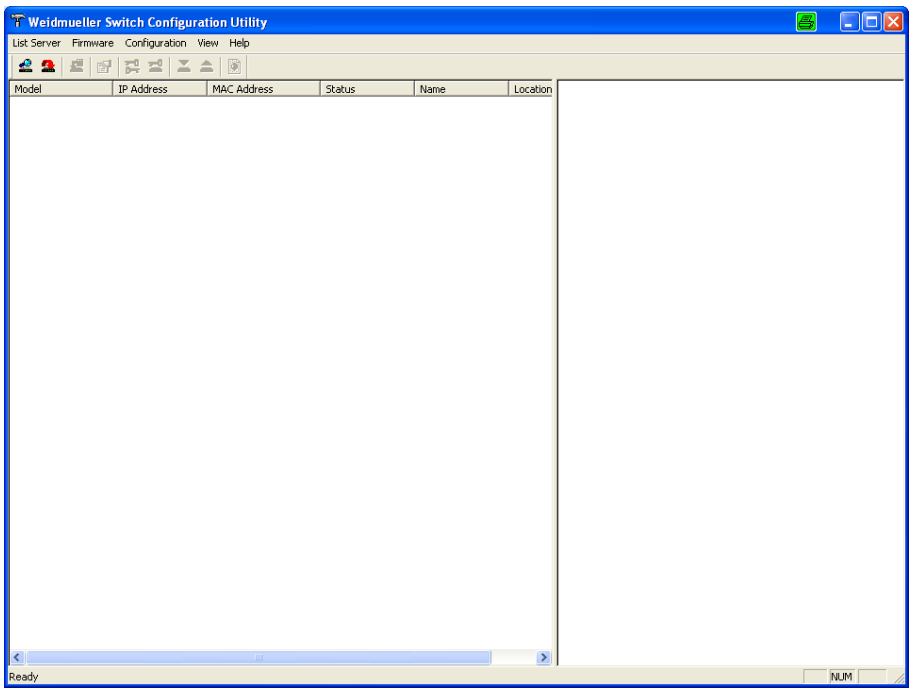
To start the software locate and then run the executable file **WM_Switch_Utility.exe**.

NOTE You may download the Weidmüller Switch Configuration Utility from the Weidmüller website using the following path:

1. Open www.Weidmueller.com/Downloads
2. Select page “Software”
3. Select page “Industrial Ethernet”
4. Select category “Value and Premium Line managed Switches – Software Tools”
5. Download “Weidmueller Switch Configuration Utility”

For example, if the file was placed on the Windows desktop, it should appear as follows. Double click the icon to run the program.

The Weidmueller Switch Configuration Utility window will open, as shown.

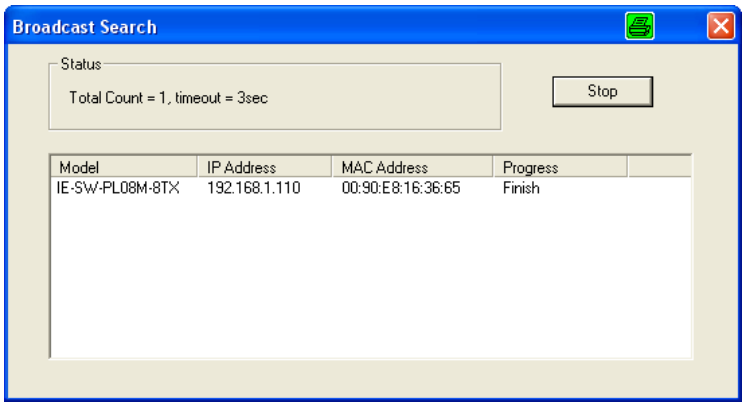


Broadcast Search

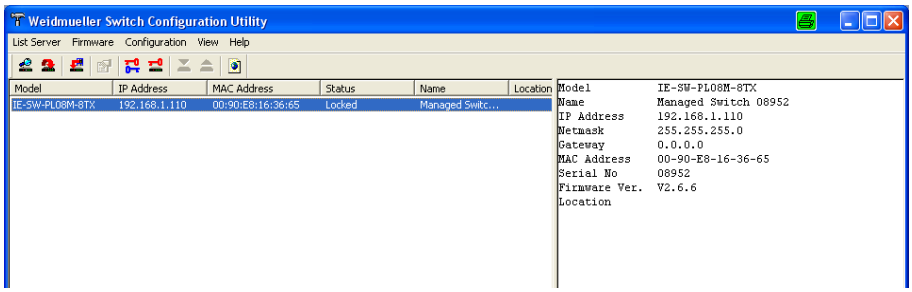
Use the Broadcast Search utility to search the LAN for all Weidmueller managed Switches that are connected to the LAN. Note that since the search is done by MAC address, Broadcast Search will not be able to locate devicess connected outside the PC host’s LAN. Start by clicking the Broadcast

Search icon, or by selecting **Broadcast Search** from the **List Server** menu.

The Broadcast Search window will open, displaying a list of all switches located on the network, as well as the progress of the search.



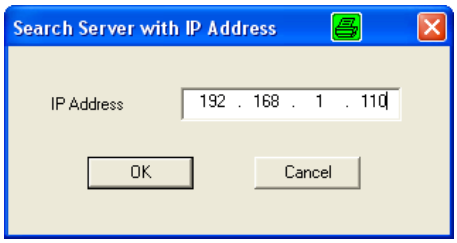
Once the search is complete, the Configuration window will display a list of all switches that were located.



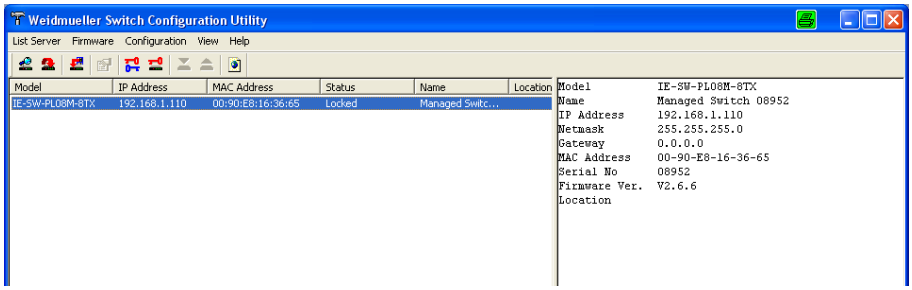
Search by IP address

This utility is used to search for Weidmueller Switches one at a time. Note that the search is conducted by IP address, so you should be able to locate any Weidmüller managed Switch which is properly connected to your LAN, WAN, or even the Internet. Start by clicking the Specify by IP address icon, or by selecting **Specify IP address** from the **List Server** menu.

The **Search Server with IP Address** window will open. Enter the IP address of the switch you wish to search for, and then click **OK**.



Once the search is complete, the Utility window will add the switch to the list of switches.



Upgrade Firmware

NOTE

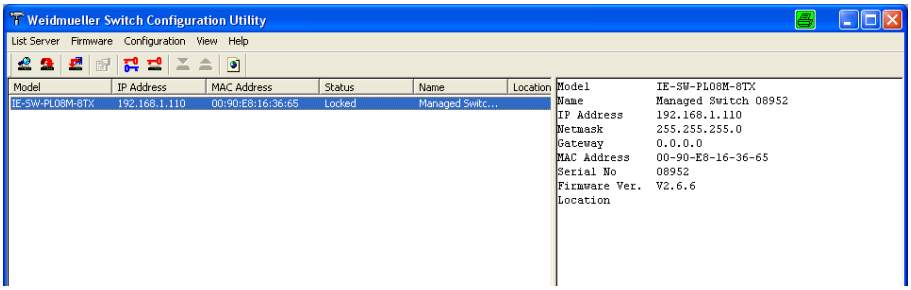
You may download the latest Firmware from the Weidmüller website using the following path:

1. Open www.Weidmueller.com/Downloads
2. Select page “Software”
3. Select page “Industrial Ethernet”
4. Select category “Value and Premium Line managed Switches – Firmware Updates”
5. Select the entry “IE-SW-VL08M-Series” for Firmware download

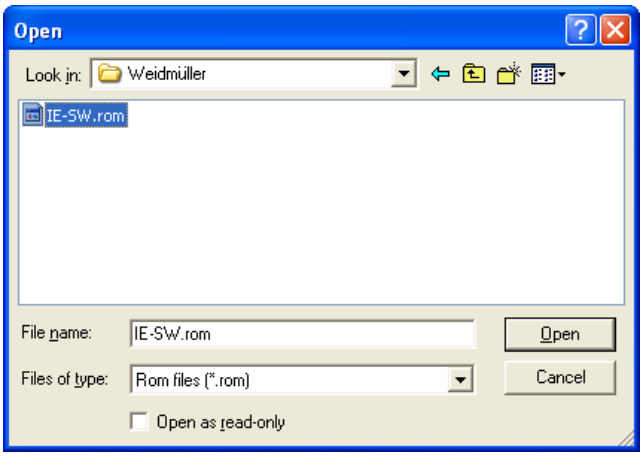
Note: The unzipped Firmware file has the extension *.rom

Keep your Weidmueller Ethernet Switch up to date with the latest firmware from Weidmueller. Do the following to upgrade the firmware:

1. Download the updated firmware (*.rom) file from the Weidmueller website as described above.
2. Click the switch (from the **Switch Configuration** window) whose firmware you wish to upgrade to highlight it.



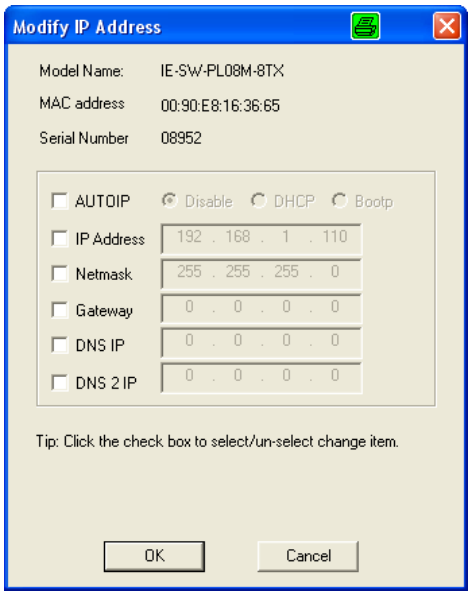
3. Click the **Upgrade Firmware** toolbar icon , or select **Upgrade** from the **Firmware** menu. If the switch is locked, you will be prompted to input the switch’s User Name and Password.
4. Click **Open** to navigate to the folder that contains the firmware upgrade file, and then click the correct “*.rom” file (**IE-SW.rom** in the example shown below) to select the file. Click **Open** to activate the upgrade process.



Modify IP Address

You may use the Modify IP Address function to reconfigure the Weidmueller Switch's network settings. Start by clicking the Modify IP address icon, or by selecting **Modify IP address** from the **Configuration** menu.

The **Setup Configuration** window will open. Select the box to the left of those items that you wish to modify, and then Disable or Enable DHCP, and enter the IP Address, Netmask, Gateway, and DNS IP. Click **OK** to accept the changes to the configuration.

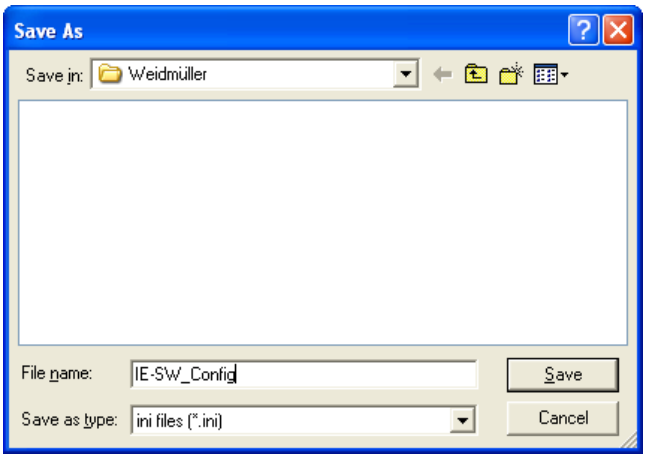


Export Configuration

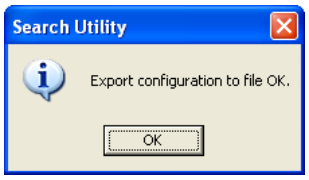
The **Export Configuration** utility is used to save the entire configuration of a particular

Weidmueller Switch to a text file. Do the following to export a configuration:

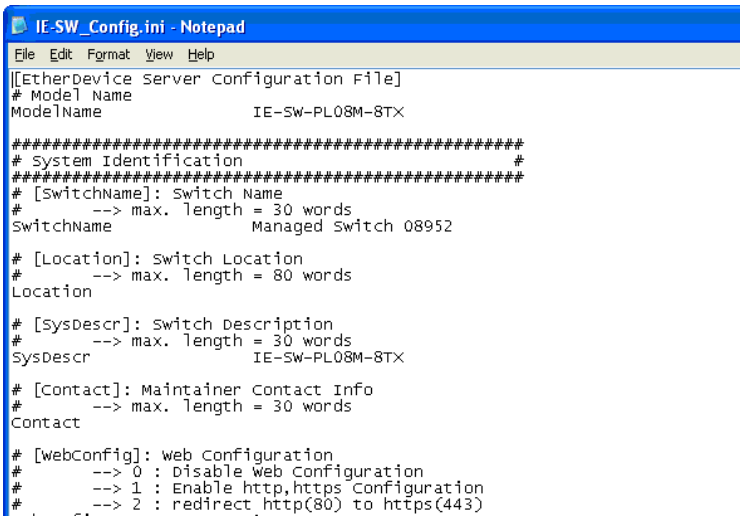
1. Highlight the switch (from the Server list in the Configurator window's left pane), and then click the **Export** toolbar icon or select **Export Configuration** from the **Configuration** menu. Click **Open** to navigate to the folder in which you want to store the configuration, and then type the name of the file in the File name input box. Click **Save** to export the configuration.



2. Click **OK** when the **Export configuration to file OK** message appears.



3. You may use a standard text editor, such as Notepad under Windows, to view and modify the newly created configuration file.

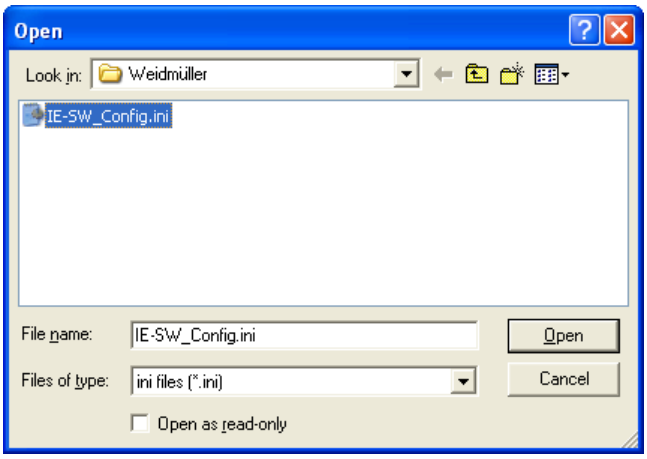

IE-SW_Config.ini - Notepad
File Edit Format View Help
[EtherDevice Server Configuration File]
Model Name
ModelName IE-SW-PL08M-8TX
##
System Identification
##
[SwitchName]: Switch Name
--> max. length = 30 words
SwitchName Managed Switch 08952
[Location]: Switch Location
--> max. length = 80 words
Location
[SysDescr]: Switch Description
--> max. length = 30 words
SysDescr IE-SW-PL08M-8TX
[Contact]: Maintainer Contact Info
--> max. length = 30 words
Contact
[WebConfig]: Web Configuration
--> 0 : Disable Web Configuration
--> 1 : Enable http,https Configuration
--> 2 : redirect http(80) to https(443)

Import Configuration

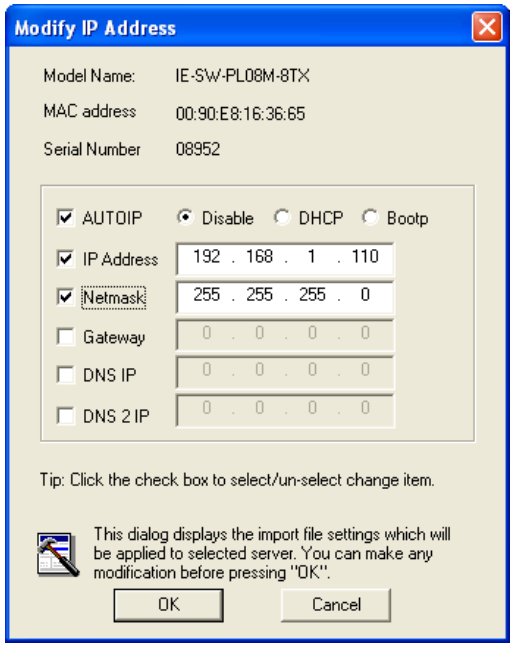
The **Import Configuration** function is used to import an entire configuration from a text file to the Switch. This utility can be used to transfer the configuration from one Switch to another, by first using the Export Configuration function (described in the previous section) to save a switch configuration to a file, and then using the Import Configuration function. Do the following to import a configuration:

1. Highlight the server (from the Weidmueller Switch list in the Configurator window's left pane), and then click the **Import** toolbar icon , or select **Import Configuration** from the **Configuration** menu.

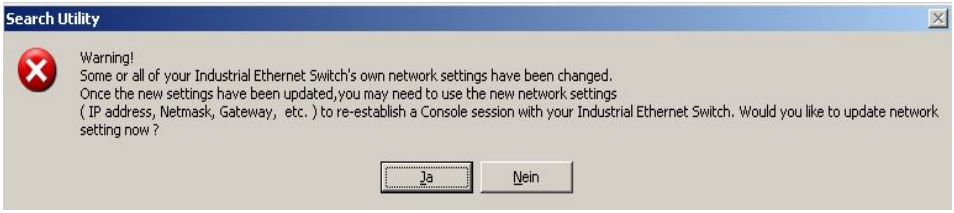
2. Click **Open** to navigate to the text file that contains the desired configuration. Once the file is selected, click **Open** again to initiate the import procedure.



3. The **Setup Configuration** window will be displayed, with a special note attached at the lower portion of the window. Parameters that have been changed will be activated with a checkmark. You may make more changes if necessary, and then click **OK** to accept the changes.



4. Click **Yes** in response to the following warning message to accept the new settings.


Search Utility
Warning!
Some or all of your Industrial Ethernet Switch's own network settings have been changed.
Once the new settings have been updated,you may need to use the new network settings
(IP address, Netmask, Gateway, etc.) to re-establish a Console session with your Industrial Ethernet Switch. Would you like to update network setting now ?
Ja
Nein

Unlock the Ethernet Switch

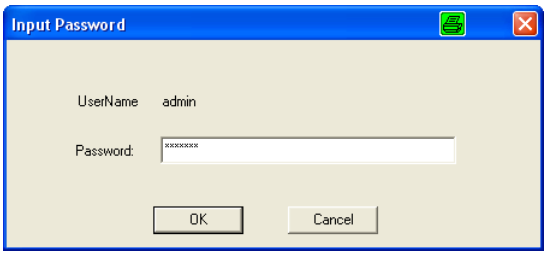
The Unlock function is used to open a password protected switch so that the user can modify its configuration, import/export a configuration, etc. There are six possible responses under the **Status** column. The **Status** of a Weidmueller Switch indicates how the switch was located (by Weidmueller Switch Utility), and what type of password protection it has.

The six options are as follows (note that the term **Fixed** is borrowed from the standard *fixed IP address* networking terminology):

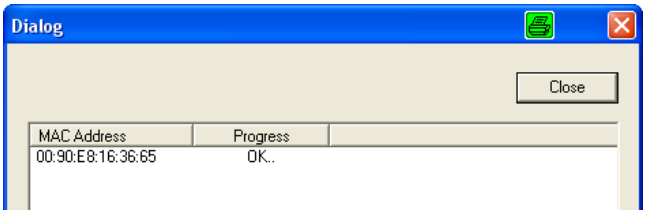
- **Locked**
  The switch is password protected, ***Broadcast Search*** was used to locate it, and the password has not yet been entered from within the current Configurator session.
- **Unlocked**
  The switch is password protected, ***Broadcast Search*** was used to locate it, and the password has been entered from within the current Configurator session. Henceforth during this Configurator session, activating various utilities for this switch will not require re-entering the server password.
- **Blank**
  The device is not password protected, and ***Broadcast Search*** was used to locate it.
- **Fixed**
  The device is not password protected, and ***Search by IP address*** was used to locate it manually.
- **Locked Fixed**
  The device is password protected, ***Search by IP address*** was used to locate it manually, and the password has not yet been entered from within the current Configurator session.
- **Unlocked Fixed**
  The device is password protected, ***Search by IP address*** was used to locate it manually, and the password has been entered from within the current Configurator session. Henceforth during this Configurator session, activating various utilities for this switch will not require re-entering the server password.

Perform the following steps to unlock a locked device (i.e., a Weidmueller Industrial Ethernet Switch with Status “Locked” or “Locked Fixed”). Highlight the server (from the Weidmueller Industrial Ethernet Switch list in the Configurator window’s left pane), and then click the **Unlock** toolbar icon , or select **Unlock** from the **Configuration** menu.

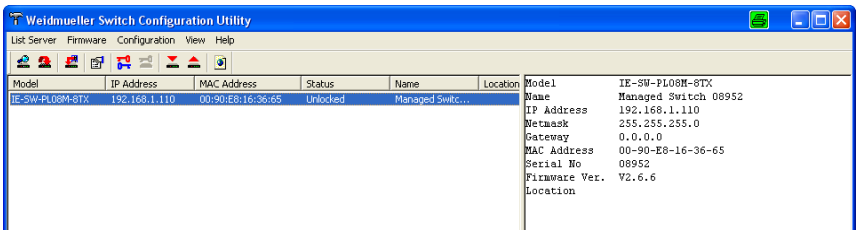
1. Enter the switch's **User Name** and **Password** when prompted, and then click **OK**.



2. When the **Unlock status** window reports Progress as **OK**, click the **Close** button on the upper right corner of the window.



3. The status of the switch will now read either **Unlocked** or **Unlocked Fixed**.



A

MIB Groups

Weidmueller Ethernet Switches come with built-in SNMP (Simple Network Management Protocol) agent software that supports cold/warm start trap, line up/down trap, and RFC 1213 MIB-II.

The standard MIB groups supported by the IE-SW-VL08M switch series are:

MIB II.1 – System Group

MIB II.2 – Interfaces Group

MIB II.4 – IP Group

MIB II.5 – ICMP Group

MIB II.6 – TCP Group

MIB II.7 – UDP Group

MIB II.10 – Transmission Group

MIB II.11 – SNMP Group

MIB II.16 – RMON

MIB II.17 – Dot1dBridge Group

MIB II.17.2 – RSTP-MIB Group

MIB II.17.6 – pBridge Group

The IE-SW-VL08M also provides a private MIB file, located in the file “IE-SW-VL08M-MIB.my” on the Utility CD-ROM or downloadable from the Weidmueller website.

B

Modbus/TCP Map

Modbus Information

Read Only Registers (Support Function Code 4) 1 Word = 2 Bytes

Address	Data Type	Description
System Information		
0x0000	1 word	Vendor ID = 0xFFFF
0x0001	1 word	Unit ID (Ethernet = 1)
0x0002	1 word	Product Code = 0x0003
0x0010	20 word	Vendor Name = "Weidmueller" Word 0 Hi byte = 'W' Word 0 Lo byte = 'e' Word 1 Hi byte = 'i' Word 1 Lo byte = 'd' Word 2 Hi byte = 'm' Word 2 Lo byte = 'u' Word 3 Hi byte = 'e' Word 3 Lo byte = 'l' Word 4 Hi byte = 'l' Word 4 Lo byte = 'e' Word 5 Hi byte = 'r' Word 5 Lo byte = ' ' Word 6 Hi byte = '\0' Word 6 Lo byte = '\0'
0x0030	20 word	Product Name = “IE-SW-VL08M” Word 0 Hi byte = ‘I’ Word 0 Lo byte = ‘E’ Word 1 Hi byte = ‘-’ Word 1 Lo byte = ‘V’ Word 2 Hi byte = ‘L’ Word 2 Lo byte = ‘0’ Word 3 Hi byte = ‘8’ Word 3 Lo byte = ‘M’ Word 4 Hi byte = ‘\0’ Word 4 Lo byte = ‘\0’
0x0050	1 word	Product Serial Number
0x0051	2 word	Firmware Version Word 0 Hi byte = major (A) Word 0 Lo byte = minor (B) Word 1 Hi byte = release (C) Word 1 Lo byte = build (D)

0x0053	2 word	Firmware Release Date Firmware was released on 2007-05-06 at 09 o'clock Word 0 = 0x0609 Word 1 = 0x0705
0x0055	3 word	Ethernet MAC Address Ex: MAC = 00-01-02-03-04-05 Word 0 Hi byte = 0x00 Word 0 Lo byte = 0x01 Word 1 Hi byte = 0x02 Word 1 Lo byte = 0x03 Word 2 Hi byte = 0x04 Word 2 Lo byte = 0x05
0x0058	1 word	Power 1 0x0000:Off 0x0001:On
0x0059	1 word	Power 2 0x0000:Off 0x0001:On
0x005A	1 word	Fault LED Status 0x0000:No 0x0001:Yes
0x0082	1 word	DO1 0x0000:Off 0x0001:On
Port Information		
0x1000 to 0x1011	1 word	Port 1 to 8 Status 0x0000:Link down 0x0001:Link up 0x0002:Disable 0xFFFF:No port
0x1100 to 0x1111	1 word	Port 1 to 8 Speed 0x0000:10M-Half 0x0001:10M-Full 0x0002:100M-Half 0x0003:100M-Full 0xFFFF:No port
0x1200 to 0x1211	1 word	Port 1 to 8 Flow Ctrl 0x0000:Off 0x0001:On 0xFFFF:No port
0x1300 to 0x1311	1 word	Port 1 to 8 MDI/MDIX 0x0000:MDI 0x0001:MDIX 0xFFFF:No port

0x1400 to 0x1413(Port 1) 0x1414 to 0x1427(Port 2)	20 word	Port 1 to 8 Description Port Description = "100TX,RJ45." Word 0 Hi byte = '1' Word 0 Lo byte = '0' Word 1 Hi byte = '0' Word 1 Lo byte = 'T' … Word 4 Hi byte = '4' Word 4 Lo byte = '5' Word 5 Hi byte = '.' Word 5 Lo byte = '\0'
Packet Information		
0x2000 to 0x2023	2 word	Port 1 to 8 Tx Packets Ex: port 1 Tx Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2100 to 0x2123	2 word	Port 1 to 8 Rx Packets Ex: port 1 Rx Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2200 to 0x2223	2 word	port 1 to 8 Tx Error Packets Ex: port 1 Tx Error Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211
0x2300 to 0x2323	2 word	port 1 to 8 Rx Error Packets Ex: port 1 Rx Error Packets = 0x44332211 Word 0 = 4433 Word 1 = 2211
Redundancy Information		
0x3000	1 word	Redundancy Protocol 0x0000:None 0x0001:RSTP 0x0002:Turbo Ring 0x0003:Turbo Ring V2 0x0004:Turbo Chain
0x3100	1 word	RSTP Root 0x0000:Not Root 0x0001:Root 0xFFFF:RSTP Not Enable
0x3200 to 0x3211	1 word	RSTP Port 1 to 8 Status 0x0000:Port Disabled 0x0001:Not RSTP Port 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:RSTP Not Enable
0x3300	1 word	TR Master/Slave 0x0000:Slave 0x0001:Master 0xFFFF:Turbo Ring Not Enable

0x3301	1 word	TR 1st Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding
0x3302	1 word	TR 2nd Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding
0x3303	1 word	TR Coupling 0x0000:Off 0x0001:On 0xFFFF:Turbo Ring Not Enable
0x3304	1 word	TR Coupling Port status 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0005:Forwarding 0xFFFF:Turbo Ring Not Enable
0x3305	1 word	TR Coupling Control Port status 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0005:Forwarding 0x0006:Inactive 0x0007:Active 0xFFFF:Turbo Ring Not Enable
0x3500	1 word	TR2 Coupling Mode 0x0000:None 0x0001:Dual Homing 0x0002:Coupling Backup 0x0003:Coupling Primary 0xFFFF:Turbo Ring V2 Not Enable
0x3501	1 word	TR2 Coupling Port Primary status (Using in Dual Homing, Coupling Backup, Coupling Primary) 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Not Enable

0x3502	1 word	TR2 Coupling Port Backup status (Only using in Dual Homing) 0x0000:Port Disabled 0x0001:Not Coupling Port 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Not Enable
0x3600	1 word	TR2 Ring 1 status 0x0000:Healthy 0x0001:Break 0xFFFF:Turbo Ring V2 Not Enable
0x3601	1 word	TR2 Ring 1 Master/Slave 0x0000:Slave 0x0001:Master 0xFFFF:Turbo Ring V2 Ring 1 Not Enable
0x3602	1 word	TR2 Ring 1 1st Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 1 Not Enable
0x3603	1 word	TR2 Ring 1 2nd Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 1 Not Enable
0x3680	1 word	TR2 Ring 2 status 0x0000:Healthy 0x0001:Break 0xFFFF:Turbo Ring V2 Ring 2 Not Enable
0x3681	1 word	TR2 Ring 2 Master/Slave 0x0000:Slave 0x0001:Master 0xFFFF:Turbo Ring V2 Ring 2 Not Enable
0x3682	1 word	TR2 Ring 2 1st Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 2 Not Enable

0x3683	1 word	TR2 Ring 2 2nd Port status 0x0000:Port Disabled 0x0001:Not Redundant 0x0002:Link Down 0x0003:Blocked 0x0004:Learning 0x0005:Forwarding 0xFFFF:Turbo Ring V2 Ring 2 Not Enable
0x3700	1 word	Turbo Chain Switch Role 0x0000:Head 0x0001:Member 0x0002:Tail 0xFFFF: Turbo Chain Not Enable
0x3701	1 word	Turbo Chain 1st Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF:Turbo Ring V2 Ring 2 Not Enable
0x3702	1 word	Turbo Chain 2nd Port status 0x0000: Link Down 0x0001: Blocking 0x0002: Blocked 0x0003: Forwarding 0xFFFF:Turbo Ring V2 Ring 2 Not Enable

Memory mapping from address 0x0000 to 0x3FFF.